VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Virtuální privátní síť
Virtual private network

2010 Roman Veřmiřovský

Prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 1. 5. 2010 . . . . . .

podpis

Poděkování

Chtěl bych poděkovat panu doc. Ing. Jaroslavu Zdrálkovi, Ph.D. za jeho vstřícný přístup a odbornou pomoc při psaní této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá bezpečným přístupem do sítě LAN, která se nachází za bezpečnostní bránou Zyxel Zywall USG 100. K tomuto přístupu jsem využil VPN. VPN je dnes velmi rozšířenou technologií a nasazuje se zejména ve firmách. Umožňuje bezpečnou výměnu informací mezi pobočkami, ale také mezi firmou a cestujícími zaměstnanci. V diplomové práci nakonfiguruji přístup přes SSL, L2TP a IPSec VPN a stručně se zaměřím i na firewall. Jednotlivé konfigurace také porovnám z hlediska administrace, bezpečnosti, nákladů na provoz a složitosti konfigurace na straně uživatele.

Klíčová slova:

Virtuální privátní síť, VPN, SSL VPN, L2TP VPN, IPSec, Zyxel Zywall USG 100

Abstract

This thesis is about secure access do the LAN, which is behind security gateway Zyxel Zywall USG 100. I use VPN for this access. Today, VPN is very used technology especially in companies with remote officess and travelling employees. In my thesis I configure access to the LAN behind Zywall throught SSL, L2TP and IPSec and I also concisely describe firewall. Then I compare these individual configurations in terms of administration, security, operating costs and the complexity of configuration for users.

Key words

Virtual private network, VPN, SSL VPN, L2TP VPN, IPSec, Zyxel Zywall USG 100

Seznam použitých zkratek

DES, 3DES, AES	Data Encryption Standard, Triple Data Encryption Standard, Advanced Encryption Standard - algoritmy pro šifrování paketů. AES je nejbezpečnější algoritmus, doposud není znám veřejný případ prolomení této metody ochrany dat.
DH	Diffie – Helmann je kryptografický protokol pro bezpečnou výměnu sdílených klíčů přes nezabezpečený kanál např. Internet
Https	Hypertext Transfer Protocol Secure – nadstavba síťového protokolu http, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje ověřit identitu protistrany, přičemž přenášená data jsou šifrována pomocí SSL nebo TLS a standardní port na straně serveru je 443.
IDS	Instrusion Detection Systém – zařízení nebo aplikace, která monitoruje síťové nebo systémové škodlivé aktivity a porušení pravidel a podává o takovémto chování hlášení na monitorovací stanici.
IM	Instant Messaging – textová forma real – time komunikace mezi dvěma a více počítači.
IP	Internet protokol – datový protokol používaný pro přenos dat přes paketové sítě.
ICSA certifikace	Certifikace americké laboratoře ICSA. Zaručuje uživateli při správné konfiguraci špičkovou úroveň zabezpečení proti vnějším útokům.
LAN	Local Area Network – místní síť – počítačová síť, která pokrývá malé geografické území (domácnosti, malé firmy).
NAT	Network Address Translation – překlad síťových adres – způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů.
MD5, SHA1	Message – Digest algorithm, Secure Shell Algorithm – hašovací funkce, které vytváří ze vstupních dat výstup fixní délky. Malá změna na vstupu vede k velké změně na výstupu.
MTU	Maximum Transmission Unit – maximální přenosová jednotka, v sadě protokolů internetu se jedná o označení maximální velikosti IP paketu.

OSI model	Model, který rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev. Je popsán v ISO 7498.
P2P	Peer – to – Peer. Označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví uživatelé.
PGP	Pretty Good Privacy – počítačový program, který umožňuje šifrování a podepisování. Je založeno na algoritmu RSA pro asymetrickou kryptografii.
PPP	Point – to – Point Protocol – komunikační protokol linkové vrstvy používaný pro přímé spojení mezi dvěma síťovými uzly. Umožňuje autentizaci, šifrování a kompresi.
TLS	Transport Layer Security - je kryptografický protokol, poskytující možnost zabezpečené komunikace na Internetu pro služby jako WWW, elektronická pošta, internetový fax a další datové přenosy.
WAN	Počítačová síť, která pokrývá rozlehlé geografické území (síť, která překračuje hranice města, regionu nebo státu). Nejznámější WAN síť je Internet.

Obsah

1. Úvod

Bezpečnost počítačových sítí je dnes velmi důležitým pojmem, se kterým se můžeme setkat tam, kde jsou počítače připojené k síti, např. Internetu. Síťovou bezpečnost lze řešit jednotlivě na počítačích, nebo hromadně zabezpečit celou síť.

Zabezpečení jednotlivých počítačů řeší zejména soukromé osoby. Avšak tyto osoby většinou této problematice nerozumí, bezpečnost svých stanic podceňují a myslí si, že útoky hackerů se jich netýkají. Často ale používají velmi důvěryhodné informace: platí na internetu platebními kartami, spravují svůj bankovní účet atd. Ale všechny tyto informace mohou být odposlouchávány třetí osobou a později zneužity. Proto je důležité, aby na svých počítačích udržovali legální a aktualizovaný operační systém, antivirový systém, personální firewall a vyhnuli se používání nezabezpečených a nevhodných služeb nebo nevhodných hesel.

Zabezpečení celých sítí řeší firmy, které musí ochránit více počítačů. Výrobní závody nebo poskytovatelé internetu řeší zabezpečení hromadně hardwarově, na rozdíl od soukromých osob, které zabezpečují softwarově. Firemní administrátoři by se měli zaměřit na bezpečnostní rizika a politiku, fyzicky zabezpečit přístup k serverům, pracovním stanicím a síťovým prvkům. Také zabezpečit pohybující se osoby s notebooky, vhodně konfigurovat firewally, aktualizovat je a zamezit zneužití citlivých informací.

Bezpečnost počítačových sítí je rozsáhlá problematika. Můžeme definovat nejrůznější pravidla pro přístup k určitým službám nebo serverům (firewall), antivirové programy, detekční systémy IDS. IDS detekuje zlomyslné nebo nežádoucí události a upozorňuje na ně. Další volbou jsou VPN přístupy, kdy určujeme s využitím šifrování a autentizace, kdo se může k síti připojit a k jakým serverům nebo stanicím. Ačkoliv jsou tyto systémy dnes velice sofistikované, vždy budou o krok zpět před hackery, kteří i přes tyto zabezpečovací metody naleznou „díru“ v síti a informace získají. Tito lidé se ale vystavují trestnímu stíhání a prevence je základní ideou bezpečné komunikace.

Tato diplomová práce se zabývá metodou bezpečného vzdáleného přístupu k síti (VPN) a základy konfigurace firewallu s využitím zařízení od firmy Zyxel Zywall USG 100.

2. Teoretický rozbor

V této kapitole popíšu co je to virtuální privátní síť, jaké protokoly se používají pro bezpečnou komunikaci na transportní, síťové a datalinkové vrstvě referenčního modelu OSI.

2.1. Úvod do VPN

Již od počátku počítačových sítí bylo potřeba bezpečně přesouvat informace z jednoho stanoviště na druhé. V minulosti byly tyto transporty prováděny soukromými linkami, které si pronajímali prodejci komunikací, takže společnosti měly privátní segment pro takovéto komunikace. Čím byla ale větší vzdálenost, tím dražší byla tato spojení. Mnohé firmy si takovýto přepych nemohly dovolit, ale nemohly zároveň bez těchto sítí existovat. S rozvojem širokopásmového připojení k Internetu se koncept tohoto připojení začal zdát nezajímavým a do popředí se dostávala technologie VPN.

Síť VPN (Virtual Private Network) je chráněné spojení v síti, vytvořené nad nechráněnými kanály, jako je Internet. K zabezpečení komunikace využívá šifrovacích nebo autentizačních technologií. Pod zkratkou VPN označujeme zařízení na obvodu sítě, která umožňují činnost takovéto chráněné relace. VPN je vhodná technologie pro obchodní partnery, pro pracovníky na cestách nebo pro práci z domova. Prostřednictvím VPN se vnější uživatel může zapojit do vnitřní sítě, jako by k ní byl připojený přímo. VPN může být vytvořena v mnoha variantách - mezi dvěma koncovými systémy, mezi dvěma organizacemi, mezi několika koncovými systémy v rámci jedné organizace nebo mezi více organizacemi pomocí např. globální sítě Internet. Může být vytvořena také přímo mezi aplikacemi a samozřejmě také libovolnou kombinací všech uvedených možností.

2.2. Typy VPN

Síť VPN lze rozdělit do tří základních typů: hostitel – hostitel, hostitel – vstupní brána (gateway), vstupní brána – vstupní brána (gateway – gateway). Komunikace může být zabezpečena na mnoha vrstvách RM OSI modelu, například na aplikační, transportní, síťové nebo datalinkové vrstvě.

Na aplikační vrstvě může být šifrování zajištěno programově, například šifrovací metodou Pretty Good Privacy (PGP) nebo pomocí zabezpečených kanálů jako je Secure Shell (SSH). Vyjma SSH, které lze použít pro vytvoření tunelu v režimu port – forwarding, pracují programy na aplikační vrstvě z hostitelského počítače na hostitelský počítač. To znamená, že nabízejí ochranu obsahu paketů, nikoliv však paketů samotného.

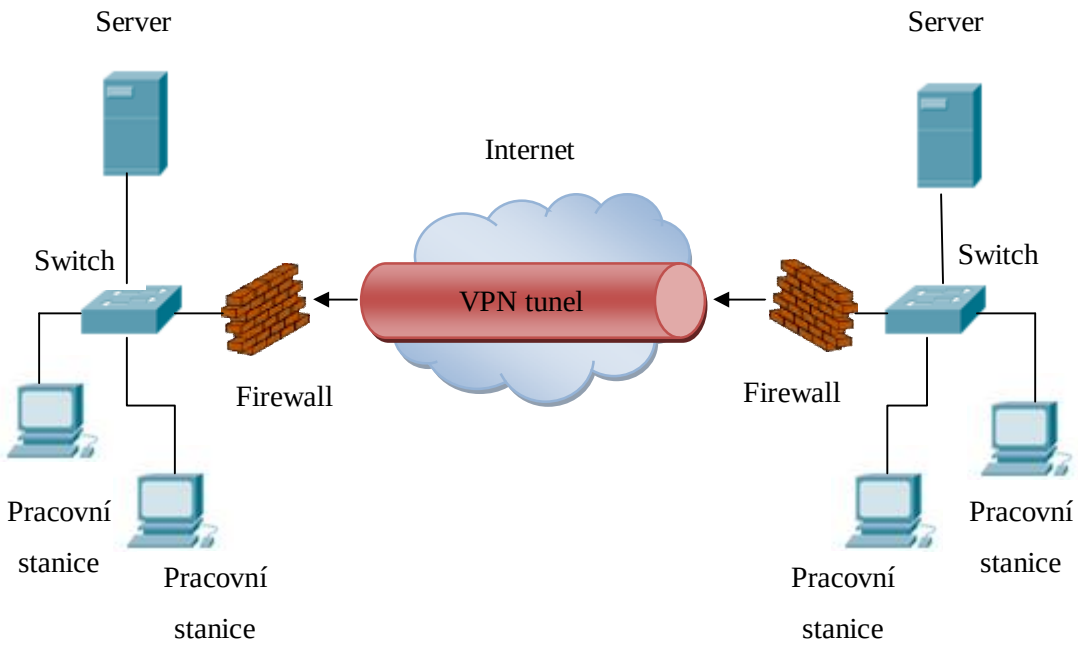
Na transportní vrstvě se používají protokoly, jako je například Secure Socket Layer (SSL), pro ochranu užitečného obsahu komunikace mezi dvěma stranami. Typicky se tento způsob zabezpečení využívá při komunikaci s webovým prohlížečem. Na této vrstvě jsou opět chráněny pouze obsahy komunikace, ale IP pakety, které tyto informace obsahují, může získat kdokoliv.

V síťové vrstvě se již nešifruje pouze užitečný obsah, ale šifrují se také TCP/IP informace. Na této vrstvě pracuje protokol IPSec. Existují dva způsoby pro bezpečnou komunikaci na této vrstvě. První způsob je nezašifrovaná IP adresa, ostatní informace z vyšších vrstev, jako je typ transportních protokolů a asociovaných portů lze kompletně zašifrovat. Druhý způsob je šifrování v konceptu „tunelování“. Pokud tento způsob umožňuje síťové zařízení jako je směrovač nebo firewall, je možné v paketu skrýt také IP adresu koncové stanice. Tunelovací protokol druhé vrstvy (Layer 2 Tunneling Protocol – L2TP) je nadstavbou tunelovacího protokolu mezi dvěma body (Point – to – Point Protocol – PPP) a umožňuje šifrování paketů zaslaných přes PPP na druhé vrstvě RM OSI modelu. Další informace v literatuře [Thomas, 2005].

2.3. Tunelování

Tunelování je zapouzdření jednoho typu paketu do jiného tak, aby umožňoval výhodný transport. Na příkladu v obr. 2.1 můžeme popsat, jak lze použít tunelování pro zašifrování. Obě sítě jsou propojeny prostřednictvím VPN a na obou koncích jsou ukončeny firewallem. Firewall překládá všechny pakety, které směřují ke vzdálené síti, do šifrované podoby a k výslednému užitečnému obsahu přidává novou IP hlavičku se svou vlastní adresou (adresa zdroje) a IP adresou vzdáleného firewallu (cílová adresa). Tímto způsobem se zašifrují skutečné IP adresy původního paketu. Jakmile vzdálený firewall takovýto paket obdrží, dešifruje jej a přepošle k hostitelskému počítači, ke kterému původně směřoval. Virtuální segment, který se takto vytvořil mezi dvěma bránami, se nazývá tunel. Hostitelský počítač není

třeba speciálně nastavovat nebo instalovat zvláštní software, protože nemusí vědět, že pakety jsou šifrovány nebo přeposílány přes veřejnou síť.



Obr. 2.1 - Tunelování

Šifrování, zapouzdření a tunelování nedělají zasílané pakety nedosažitelnými. Pakety může stále někdo shromažďovat a analyzovat. Pokud jsou ale tyto metody dobře realizovány a používá se silný šifrovací algoritmus, užitečný obsah paketů by měl zůstat zabezpečený.

2.4. Výhody a nevýhody VPN

Hlavní výhodu VPN je, že můžeme využít veřejně dostupný prostředek k přenosu privátních informací. VPN může obsahovat celou řadu úrovní bezpečností pro sdílení síťového média, včetně zlepšování důvěryhodnosti, integrity a autentičnosti.

Součástí sítě VPN jsou bezpečnostní prvky, které dělají tyto sítě efektivní pro zabezpečení komunikace. Bez ohledu na to, jak odolnou šifrovací technologii používáme, měla by síť splňovat další požadavky tak, aby se jednalo skutečně o zabezpečený komunikační kanál.

Nejzásadnější jsou:

1. Utajení – nikdo jiný nebude schopen nahlédnout do našich informací, tuto funkci zajišťují šifrovací algoritmy.
2. Integrita dat – zaručuje, že odeslaná data jsou stejná jako data přijatá. Integritu zajišťují digitální podpisy a hash (hašovací funkce)
3. Autentičnost – ověření, odkud informace opravdu pochází a přijde uživateli, kterého jsme vybrali.

Další nespornou výhodou je efektivnost nákladů. Největší úspory dosáhneme, pokud nahradíme velmi drahé vyhrazené linky WAN sítí VPN. To znamená úspory v účtech vzdálených uživatelů, protože odpadá potřeba vyhrazených serverů.

VPN má ale i stinné stránky. Šifrování zatěžuje výkon bezpečnostní brány komplikovanými matematickými výpočty. Čím silnější je šifrovací mechanizmus, tím větší je omezení rychlosti. Další problém je režie spojená s pakety. Pakety se zapouzdřují a přidávají se další informace do záhlaví, což může způsobit problémy. Pokud tyto pakety přesáhnou určitou délku, zařízení je začnou fragmentovat a to negativně ovlivňuje rychlosti sítě. Při realizaci VPN je také potřeba mít určité znalosti. Někdy můžeme realizovat VPN přes NAT (problém s překladem IP adres), musíme dát pozor na maximální velikost přenosové jednotky (MTU), problémy může způsobit návrh sítě atd. Další informace lze nalézt v literatuře [Northcutt, 2005].

2.5. Protokolový balíček IPSec

Pomocí IPSec protokolu lze vytvářet VPN typu “bod – bod” i „klient – server”. Velkou výhodou IPSecu je mechanismus zabezpečení paketu, který může být šifrován kryptovacím mechanismem (DES, 3DES, AES, …) a ověřen pomocí SHA-1, nebo MD5.

Hlavním cílem zavedení protokolu IPSec bylo zajištění důvěryhodnosti (utajení), integrity a autentizace informací přenášených pomocí protokolu IP. Tato kritéria jsou splněna s použitím několika dalších protokolů, jako je systém pro výměnu klíčů IKE (Internet Key Exchange), protokol ESP (Encapsulating Security Payload) a protokol AH (Authentication Header). Kombinace těchto protokolů umožňuje bezpečnou výměnu informací bez možnosti, že by třetí strana mohla naslouchat nebo manipulovat s přenášenými daty.

SA (bezpečnostní asociace) je ustanovení mezi dvěma entitami, které udává, jak si budou mezi sebou bezpečně předávat informace. IPSec je otevřený protokol, což je jeho velká výhoda, protože podporuje rozmanité protokoly a komunikační režimy, šifrovací algoritmy a hašovací funkce. Všechny tyto detaily se vyjednávají předtím, než začne výměna uživatelských

dat. Výsledná shoda se pak nazývá SA (Security Association). Každá komunikační relace má dvě asociace SA – pro každou stranu jednu. Každý účastník si musí sjednat novou SA pro každé IPSec spojení. Než dojde k vyjednání asociace SA, musí se nastavit podrobnosti, které bude druhá strana přes IPSec podporovat. Toto nastavení se uchovává v databázi SPD (Security Policy Database). Aby mohl proces správně fungovat, musí mít každá SA relace jedinečný identifikátor. Tento identifikátor se vytvoří z parametru SPI (Security Parametr Index). SPI identifikuje položku v databázi SA odpovídajícímu spojení, cílové adresy spojení a z ukazatele na hlavičku ESP nebo AH, podle toho, který je použit.

U spojení IPSec rozlišujeme dva základní módy: transportní a tunelovací. Transportní mód je komunikace typu bod – bod a šifruje se při něm pouze užitečný obsah paketů. Při tomto módu musí být na koncových stanicích nainstalován speciální software. Tento mód je vhodný pro šifrování komunikace mezi počítači ve stejné síti, neexistuje však možnost komunikace na úrovni bezpečnostní brána – bezpečnostní brána a nelze skrýt IP informace o hostitelském počítači.

Druhý mód IPSec spojení je tunelovací mód. Tento mód je vhodnou volbou pro většinu VPN sítí, protože šifruje nejen užitečný obsah paketu, ale také celý paket. Může tak částečně nebo úplně skrýt IP adresy zdroje a cíle. Další výhodu je, že tunelovací mód lze použít pro spojení host – host, host – bezpečnostní brána a bezpečnostní brána – bezpečnostní brána. Na koncových počítačích se nemusí instalovat speciální software, stačí vhodně nastavit bezpečnostní bránu, například směrovač nebo firewall.

Protokol IKE (Internet Key Exchange) slouží při IPSec pro ověření pravosti a působí také jako zprostředkovatel spojení. IKE ověřuje, zda jste skutečně osoba, které by se mělo umožnit začít šifrovaně komunikovat s dotyčným zařízením. IKE je kombinací dvou protokolů: Security Association (protokolu Key Management, ISAKMP), který odpovídá za sjednání zabezpečení a Oakley (pozměněný Diffie – Hellman), který zodpovídá za výměnu klíčů. Vytvoření asociace SA předcházejí dvě fáze protokolu IKE:

1. Fáze 1 – dochází k autentizaci vzdáleného uživatele a k přenosu veřejného klíče, který se bude používat pro šifrování ve Fázi 2.
2. Fáze 2 – dochází ke sjednávání parametrů pro asociaci SA protokolu IPSec.

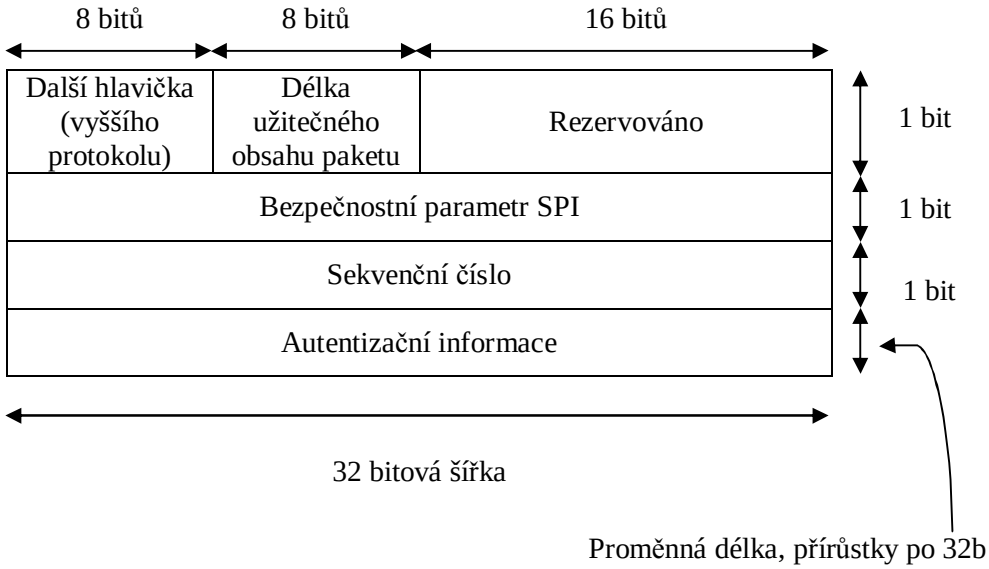
Fáze 1 – Autentičnost v protokolu IKE lze zabezpečit několika způsoby. Nejběžnější je metoda předem dohodnutých klíčů nebo metoda digitálních certifikátů. Předem dohodnuté klíče je metoda jednoduchá a efektivní. Jedná se o nejjednodušší způsob, jak nastavit autentizaci

přes VPN. Někdy se stejné klíče používají na všech komunikačních zařízeních, protože je to nejsnadnější z hlediska správy. Jelikož jsou tyto hodnoty nastaveny na místních zařízeních, může se stát, že bude narušena bezpečnost VPN spojení. Pokud je útočník dostatečně chytrý, může po sobě vymazat všechny stopy a zanechat si tak zadní dvířka do systému tak dlouho, dokud bude klíč platný. Dalším problémem je, že klíče se nastavují ručně, což může být problém ve firmě. Pokud zaměstnanec opustí firmu, administrátoři by měli změnit všechny klíče, ke kterým měla tato osoba přístup tak, aby se nemohl nadále do firemní sítě připojit. Dalším problémem je jak poslat klíče na systémy, které se spravují vzdáleně nebo komu tyto hodnoty svěřit. Druhým způsobem pro výměnu klíčů jsou digitální certifikáty. Certifikáty mohou být přiřazeny jednotlivě ke každé entitě, která se připojuje k VPN, certifikáty lze vzdáleně řídit a spravovat přes centralizovanou certifikační autoritu (CA).

Fáze 2 – Dochází ke sjednávání parametrů pro asociaci SA protokolu IPSec. Výměna informací je obdobná, jako ve Fázi 1. Teprve po dokončení Fáze 2 je vytvořena asociace SA protokolu IPSec, tedy celkového spojení VPN. Všechny výměny ve Fázi 2 jsou šifrovány stanovenými typy protokolů a šifrovacích algoritmů. Jedinou další ochranou jsou hashe, které jsou do paketů zahrnuty, aby potvrdily jejich původ.

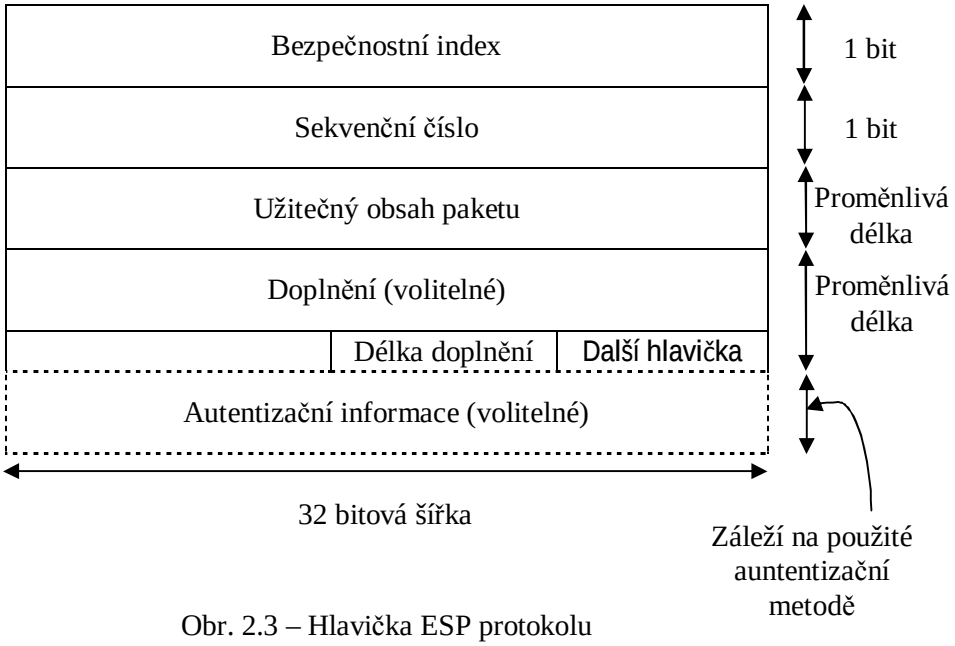
Ve skupině IPSec jsou dva zabezpečovací protokoly: AH a ESP. Při budování VPN můžeme vybrat jeden z uvedených protokolů nebo můžeme použít oba najednou. Každý má své specifické funkce, ale dnes je více používaný protokol ESP.

Protokol AH je bezpečnostní protokol, který zabezpečuje autentičnost a ověřování integrity, ale neumí zajistit důvěryhodnost užitečného obsahu paketů. Autentičnost a integritu zajišťuje přidáním další hlavičky do IP datagramu. Hlavička obsahuje digitální podpis neboli kontrolní integritní hodnotu, která je hashem a ověří tak, zda nedošlo při přenosu paketu ke změně obsahu. IP informace v paketu jsou správné, ale nejsou žádným způsobem skryty. AH protokol také umožňuje použití sekvenčních čísel, která pomáhají zabránit útokům založených na opakování paketů. Vzhledem k tomu, že AH protokol nezajišťuje důvěryhodnost, není zapotřebí dalších výpočtů pro šifrování paketů. Díky tomu jsou zařízení méně zatížená a celková velikost zabalených paketů je menší. Na obr. 2.2 lze vidět jednotlivá pole hlavičky AH protokolu.



Obr. 2.2 – Hlavička AH protokolu

Druhým bezpečnostním protokolem je ESP. Zajišťuje plnou důvěryhodnost kompletním šifrováním užitečného obsahu IP paketů. Protokol může obsahovat jakýkoliv počet symetrických šifrovacích algoritmů. ESP pracuje poněkud jinak než AH. V transportním módu ESP přidá vlastní hlavičku nad IP hlavičku a šifruje zbývající informace od čtvrté vrstvy výše. Pokud se během sjednávání IPSec spojení specifikuje autentizační služba, přidá se k paketu informace ověření, které zajistí integritu paketu a autentizaci. ESP protokol v transportním módu nelze použít pro NAT. V tunelovacím módu zabalí ESP celý původní paket a to tak, že jej zašifruje a vytvoří novou IP a ESP hlavičku. I zde se přidávají informace nutné pro autentizaci. Tunelovací mód lze použít pro NAT. U obou módu se připojuje do každého paketu sekvenční číslo, které je jako u protokolu AH ochranou proti útokům. Struktura hlavičky ESP protokolu je vyobrazena na obr. 2.3. Další informace v literatuře [Lockhart, 2005].



Obr. 2.3 – Hlavička ESP protokolu

2.6. PPTP a L2TP protokoly

Protokol IPSec není jedinou sadou tunelovacích protokolů pro VPN. Na druhé vrstvě referenčního modelu OSI se nejčastěji využívají protokoly PPTP (Peer to Peer Tunneling Protocol) a L2TP (Layer 2 Tunneling Protocol). Tyto protokoly jsou velice populární, protože jsou podporovány systémem Windows.

PPTP je důsledkem protokolu PPP. Začal se objevovat s příchodem vytáčeného přístupu na Internet. Pro šifrování používá MPPE (Microsoft Point – to – Point Encryption), který využívá šifru RC4. Protokol měl nedostatečně bezpečné autentizační metody. PPTP funguje prostřednictvím dvou kanálů, které pracují společně. První je kontrolní a řídí vlastnosti relace spojení. Druhý kanál zapouzdřuje data a využívá protokolu GRE (Generic Routing Encapsulation). Výhodou GRE je, že může zabalit a přenést pakety i jiných protokolů, než je IP. U PPTP nedochází k uváznutí v mechanizmu NAT, protože změny, které provádí NAT, se netýkají druhé vrstvy. Protokol se také může používat na mnoha hardwarových zařízeních. Na druhou stranu může být tento protokol zranitelný a být citlivý na útoky man – in – the – middle, protože pro zahájení komunikace se využívá protokol PPP.

L2TP je definován v RFC 2661 a jedná se o tunelování na druhé vrstvě. Protokol je kombinací L2F společnosti Cisco a protokolu PPTP, přičemž se snaží zkombinovat výhody těchto dvou protokolů. L2TP nahrazuje PPTP v dostupných protokolech, ze kterých se vybírá při vytváření VPN tunelů v operačních systémech Microsoft Windows. Podobně jako PPTP, používá L2TP pro autentizaci uživatele funkce protokolu PPP (MSCHAP, CHAP, EAP, PAP). Také existují dva typy komunikačních metod: řídicí zprávy a zprávy procházející přes tunel pro přenos dat. Tyto dva typy komunikace se rozlišují podle prvního bitu hlavičky protokolu PPTP. Řídicí zprávy mají přednost před datovými. Koncept v pozadí operací protokolu L2TP je obdobný jako v případě PPTP. Řídící spojení nastaví tunel, poté následuje zahájení relace. Až jsou obě fáze kompletní, informace ve tvaru rámců protokolu PPP mohou začít procházet tunelem.

2.7. Srovnání protokolů PPTP, L2TP a IPSec

Protokol L2TP je nejčastěji používán pro transport všech svých paketů (UDP port 1701). Protože je UDP nespojový protokol, může komunikace zabrat méně prostředků, než v případě PPTP, který přenáší řídicí zprávy v protokolu TCP. Výhodou L2TP oproti PPTP i IPSec je možnost vytváření vícenásobných tunelů mezi dvěma hostitelskými počítači. Podobně jako PPTP i L2TP protokol podporuje přenosy paketů jiných protokolů než IP, což je také výhoda oproti IPSec. Nevýhodou protokolu L2TP je, že se spoléhá na PPP a může se lehce stát obětí útoku man – in – the – middle. I když L2TP postrádá možnost vlastního šifrování, může pracovat ve spojení s IPSec. L2TP lze také využít pro zajištění tunelu pro transportní mód přenosů IPSec. Další informace v literatuře [Northcutt, 2005].

2.8. SSL VPN

SSL VPN je druh technologie VPN, který využívá k zabezpečení dat protokolu TLS a je dostupná přes webový prohlížeč a protokol https. SSL VPN umožňuje uživatelům připojeným k internetu vytvořit bezpečný přístup do privátní sítě. SSL pracuje mezi transportní (TCP – port 443) a aplikační vrstvou TCP/IP modelu. Oproti klasickému IPSec VPN přístupu nemusí být na koncové stanici nainstalován žádný speciální software. Firemní

uživatelé se takto mohou dostat k důvěrným firemním informacím a souborům jednoduše přes webový prohlížeč s certifikátem nebo uživatelským jménem a heslem. SSL funguje na principu klient – server. Zabezpečuje autentizaci, důvěrnost a integritu dat. Hlavním přínosem SSL VPN je, že uživatelé, kteří často cestují, se mohou k informacím dostat odkudkoliv: z vlastního notebooku, mobilního zařízení nebo kiosku v kavárně. Existují 3 druhy přístupu do SSL sítě:

1. Clientless – klient potřebuje pro přístup pouze webový prohlížeč, ale zabezpečena je pouze webová komunikace.
2. Thin client – klientův webový prohlížeč je doplněn o Java nebo ActivX applet. Tímto je zabezpečena i ne – webová komunikace (SMTP, POP3, Telnet, ping…).
3. Network client – zabezpečuje většinu typů provozu, ale klient musí mít nainstalován speciální software, který lze automaticky stáhnout z SSL serveru.

Další informace v literatuře [Odom, 2008] a v [SSL VPN].

3. Konfigurace VPN

V diplomové práci budu navrhovat laboratorní cvičení pro studenty na zařízení Zyxel Zywall USG 100. Jedná se o IPSec VPN, L2TP VPN, SSL VPN a firewall.

První laboratorní úloha bude mít za úkol konfiguraci SSL VPN a zabezpečení provozu pouze do firemní sítě. V tomto případě je nutné sestavit dvě propojené sítě. V první síti bude uživatel, který se chce dostat k firemním informacím a v druhé síti bude bezpečnostní brána Zyxel a za ní firemní servery a stanice. Uživatel, kterému bude přiděleno přihlašovací jméno a heslo se na bezpečnostní bránu přihlásí a podle zvoleného režimu SSL VPN se dostane buď pouze na servery (režim SSL proxy) nebo k serverům i stanicím (SSL full tunnel režim). Konfigurace se může otestovat dotazem na jeden ze serverů a ze zachyceného provozu bude možné vysledovat pro útočníka nepoužitelná zašifrovaná data.

Zadáním druhé laboratorní úlohy bude sestavit IPSec tunel mezi dvěma routery. Není zde šifrován provoz na internet ale pouze z privátní sítě za Zywallem a druhým routerem. Touto konfigurací simuluji připojení pro firmy, která má dvě pobočky a chce mezi nimi bezpečně posílat důvěrné informace. Pro tuto úlohu je potřeba nakonfigurovat dvě vzájemně propojené privátní sítě a v každé z nich alespoň jeden počítač. Dále je nutné mít předem správně nakonfigurovaný druhý router a podle něj provést konfiguraci Zywallu. Ověření konfigurace lze provést s programem Wireshark a příkazem ping, kde student uvidí zapouzdřené pakety ESP protokolem pro komunikaci mezi privátními sítěmi a ostatní provoz nezabezpečený.

Třetí částí bude nastavení IPSec tunelu pro mobilního uživatele. Tento uživatel bude vstupovat do privátní sítě k firemním serverům a stanicím z internetu. V tomto případě bude zabezpečen veškerý provoz. Pokud bude uživatel vstupovat na internet, bude využívat veřejné IP adresy bezpečnostní brány a bude chráněn firemním antivirovým systémem a firewallem. Tato konfigurace ale vyžaduje placený software Zyxel Zywall IPSec klient. Lze stáhnout zkušební verzi na 30 dní, ale po uplynutí této doby není možné program dále využívat. Proto tuto konfiguraci doporučuji provádět na ukázku pouze jednou v rámci studijní skupiny. Konfigurace se může otestovat dotazem na web server ve firemní síti nebo jakýkoliv jiný server v internetu. Z Wiresharku lze poté vysledovat zabezpečený veškerý provoz.

Čtvrtá úloha bude zaměřena na L2TP VPN. Vlastnostmi je podobná třetí úloze, na rozdíl od ní využívá další protokol – L2TP. Provoz je šifrován jak to privátní sítě, tak na internet. Na rozdíl od třetí úlohy se konfigurace na straně klienta provádí přímo ve Windows.

Obdobně lze také provoz otestovat dotazem na server v síti za bezpečnostní branou nebo na internetu.

V páté části se zaměřím na základní konfiguraci firewallu. Zde můžu zakázat služby, které by mohly být nebezpečné pro síť. Provoz lze omezit IP adresami, mohu pravidlo nastavit pro hardwarový port a zvolit různé aplikace, které budou dostupné nebo omezeny. Pro jednoduchost jsem uvedl pravidlo pro FTP. Z vnitřní sítě Zywall odepře přístup na FTP servery. Pokud někdo bude chtít vstoupit na FTP server, bezpečnostní brána tento dotaz zaznamená do logu.

3.1. Zyxel Zywall USG 100

Bezpečnostní brána Zywall USG 100 od firmy Zyxel je vhodná pro malé kanceláře nebo domácí použití. Zařízení obsahuje:

1. Stavový firewall s certifikací ICSA, který chrání síť a důležité internetové služby, např. e – mail, prohlížení internetových stránek, servery a přenos souborů.
2. Ochranu před viry a spywarem antivirovým programem Zyxel s certifikací ICSA nebo programem od Kaspersky Labs.
3. Modul IDP pro ochranu sítě před neautorizovanými průniky, jako jsou trojské koně a červy.
4. IPSec VPN pro bezpečné připojení k pobočkám, partnerům a centrálám. SSL nebo L2TP VPN pro práci z domova a bezpečné připojení k podnikové síti bez potřeby instalovat VPN software.
5. Funkci Application Patrol pro nastavení oprávnění k používání IM a P2P aplikací.
6. Antispamovou funkci k označení a zneškodnění nevyžádaných reklamních nebo škodlivých emailů.
7. Individuální konfigurace k řízení přístupu k aplikacím a zdrojům a spouštění bezpečnostních skenů na bázi uživatele nebo skupin.
8. Řízení šířky pásma pro nastavení priorit u časově náročných aplikací jako je VoIP nebo video konference.

9. Několik WAN portů pro připojení k několika poskytovatelům za účelem vyvážení datového provozu, optimalizace šířky pásma a záložní trasy v případě výpadku jednoho z poskytovatelů.
10. Rozšiřovací kartový slot a USB porty pro několik bezdrátových připojení 3G WAN.
11. Na přední a zadní straně bezpečnostní brány se nachází různé typy portů pro připojení např. WAN sítě, LAN sítě nebo DMZ serverů, viz obr. 3.1, obr. 3.2, tabulka 3.1 a tabulka 3.2.
    Další informace lze nalézt v [Zywall USG 100 User's Guide].

Obr. 3.1 – Zywall USG 100 – pohled zepředu

Obr. 3.2 – Zywall USG 100 – pohled zezadu

Port	Označení	Funkce
P1	WAN1	Pro připojení k internetu k 1. poskytovateli
P2	WAN2	Pro připojení k internetu ke 2. poskytovateli
P3	LAN1	Připojení do sítě LAN1
P4	LAN1	
P5	LAN1	
P6	WLAN	Port pro připojení bezdrátového access pointu
P7	DMZ	Port pro připojení serverů
1	USB	Porty pro připojení k dalšímu poskytovateli
2		
AUX		
Extension card slot		
Power 12VDC		Napájecí konektor
Reset		Hardwarový reset

Tabulka 3.1 – Popis portů na bezpečnostní bráně

LED	Barva	Stav	Funkce
PWR		Nesvítí	Bezpečnostní brána je vypnuta
	Zelená	Svítí	Bezpečnostní brána je zapnuta
	Červená	Svítí	Hardwarová chyba
SYS	Zelená	Nesvítí	Bezpečnostní brána není připravena k provozu
		Svítí	Bezpečnostní brána je v provozu
		Bliká	Bezpečnostní brána se restartuje
AUX	Zelená	Nesvítí	AUX port není připojen
		Bliká	AUX port přijímá nebo odesílá pakety
		Svítí	AUX port je připojen
P1 - P7	Zelená	Nesvítí	Na portu není žádný provoz
		Bliká	Port přijímá nebo odesílá pakety
	Oranžová	Nesvítí	Port není připojen
		Svítí	Port je připojen
Card	Zelená	Nesvítí	Ve slotu není karta
		Svítí	Ve slotu je karta
		Bliká	Karta ve slotu přijímá nebo odesílá data

Tabulka 3.2 – Popis funkcí LED diod na Zyxel Zywall USG 100

3.1.1. Základní konfigurace bezpečnostní brány

Pro správnou funkci bezpečnostní brány a konfiguraci dalších služeb je nutné provést nastavení připojení k internetu (pokud připojení budeme využívat), IP adres vnitřních sítí, firewallu a pro VPN konfigurovat uživatele a podsítě, které budu později potřebovat. Jelikož základní nastavení není cílem této diplomové práce, uvedu jej velmi stručně.

Nejprve se na bezpečnostní bránu přihlásím pod IP adresou 192.168.1.1, jménem admin a heslem 1234. V prvním kroku po prvním přihlášení je doporučeno změnit pro administrátora heslo. Kliknu na Object, User/Group a u uživatele admin kliknu na Edit. V poli Password a Retype zadám nové heslo a kliknu na OK. V dalším kroku se připojím k internetu nebo k sousednímu routeru. Pro laboratorní úlohy využívám připojení přes wan port k sousednímu routeru, není tedy možné vstupovat na internet. Šifrování veškerého provozu lze využít pouze v případě, kdy uživatel vstupuje na bezpečnostní bránu z internetu. IP adresy lze konfigurovat manuálně nebo přiřazovat DHCP serverem. Využiji konfiguraci IP adres přiřazovanou DHCP serverem. Kliknu na Network, Interface, Status a v řádku wan1 kliknu na Edit. Zaškrtnu pole Enable Interface, kterým port zapnu, v sekci IP Address Assignment kliknu na Get Automatically a následně na tlačítko OK. Připojení k internetu je tímto nastaveno.

Dále zvolím rozsah IP adres pro místní síť LAN1. Kliknu na Network, Interface, Status, lan1 a na tlačítko Edit. Zvolím novou IP adresu pro bezpečnostní bránu v poli IP Address Assignment a to 172.16.1.100/24. Dále v sekci DHCP Settings zvolím v DHCP, DHCP Server, IP Pool Start Address – volba první IP adresy pro klienty v síti, v mém případě 172.168.1.2, Pool Size – maximální počet přiřazených IP adres na např. 150 a First a Second DNS Server zvolím na From ISP. V další části Static DHCP Table jsem definoval dvě IP adresy, které se přiřazují k zvoleným Mac adresám a to z důvodu nastavení web a file serveru pro SSL VPN. Kliknu na OK a síť LAN1 je nastavena.

Nyní nakonfiguruji uživatele a rozsahy IP adres, které budu potřebovat pro VPN. Kliknu na Object, User/Group a na tlačítko Add. User Name na Student, User Type na User, Password a Retype na kat440. Ostatní hodnoty mohu ponechat a kliknu na OK. V sekci Object, Address nakonfiguruji SSL_Subnet, Type Subnet a rozsah na 172.16.1.0/24, LAN1_SUBNET na Type INTERFACE SUBNET a rozsah na 172.16.1.0/24, L2TP_POOL na Type Range a rozsah na 172.16.1.1 – 172.16.1.254 a L2TP_host na Type Host a adresu 0.0.0.0.

Uživatelé přistupující např. k SSL VPN z internetu se při základním nastavení na bezpečnostní bránu nedostanou. Proto je nutné zakázat, nebo smazat pravidlo pro přístup

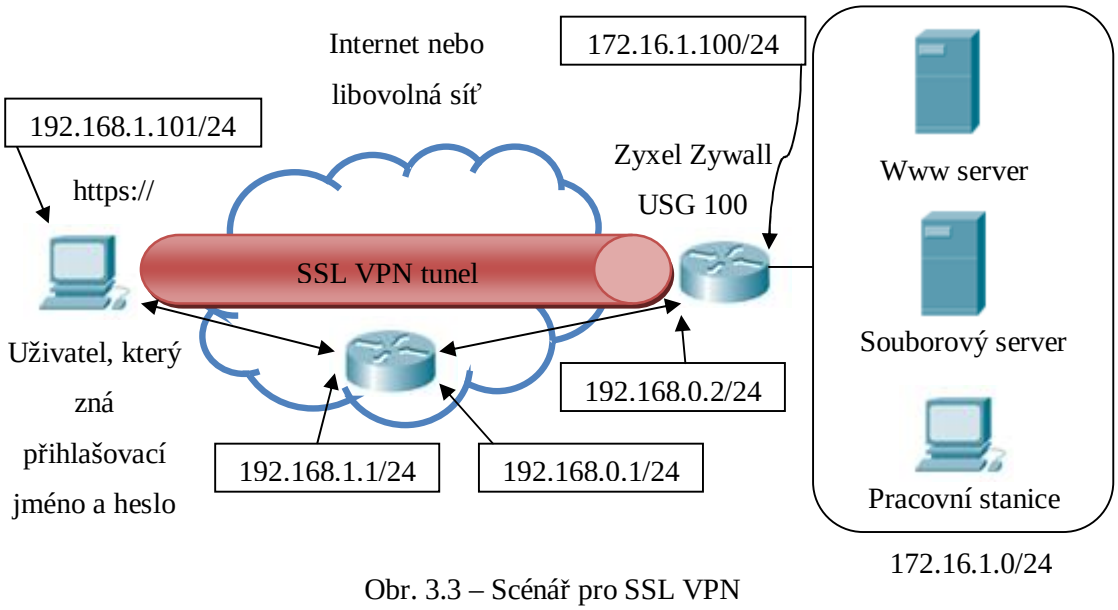
z internetu na Zywall. Vyberu položku Firewall a vypnu pravidlo pro přístup jakéhokoliv uživatele z jakoukoliv IP adresou, který přistupuje na Zywall přes WAN. Pokud provedu jakoukoliv změnu v nastavení bezpečnostní brány a chci sledovat, kdo přistupuje na Zywall, zda vytváření VPN tunelu proběhlo v pořádku nebo v některé fázi proběhla chyba, kliknu na Maintanance, Log. Zde mohu tyto funkce sledovat, filtrovat je, nebo si je pravidelně nechat posílat na e – mail.

Tímto je základní konfigurace hotová a mohu pokračovat v konfiguraci jednotlivých typů VPN.

3.2. Konfigurace SSL VPN

SSL VPN v případě zařízení Zywall USG 100 je řešeno přes webový prohlížeč a protokol https. Jednoduše řečeno, uživatel k bezpečnému připojení k síti potřebuje pouze webový prohlížeč a znát přihlašovací jméno a heslo. Na bezpečnostní bráně pak stačí nastavit, k jakým službám mají jednotliví uživatelé povolen přístup.

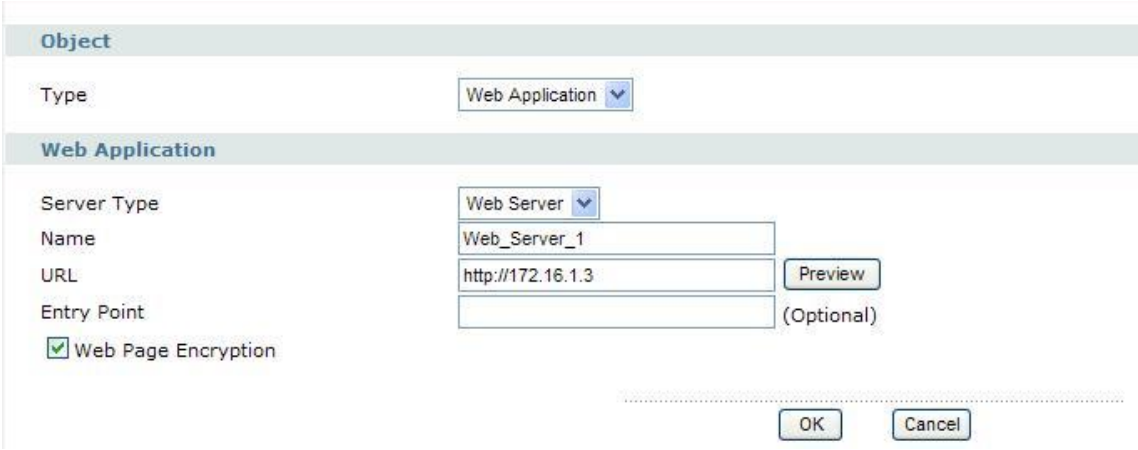
SSL VLP budu nastavovat na následujícím scénáři (obr. 3.3). Na straně Zywallu na portu Lan 1 mám připojenou síť s rozsahem 172.16.1.0/24, web server (stačí základní konfigurace serveru Apache v systému Linux) a počítač, na kterém mám nastaveno sdílení souborů jak pro čtení, tak pro zápis (souborový server). V reálném prostředí bych pro připojení k bezpečnostní bráně využil internet. V případě laboratorní úlohy propojím počítač uživatele a Zywall přes další router.



Obr. 3.3 – Scénář pro SSL VPN

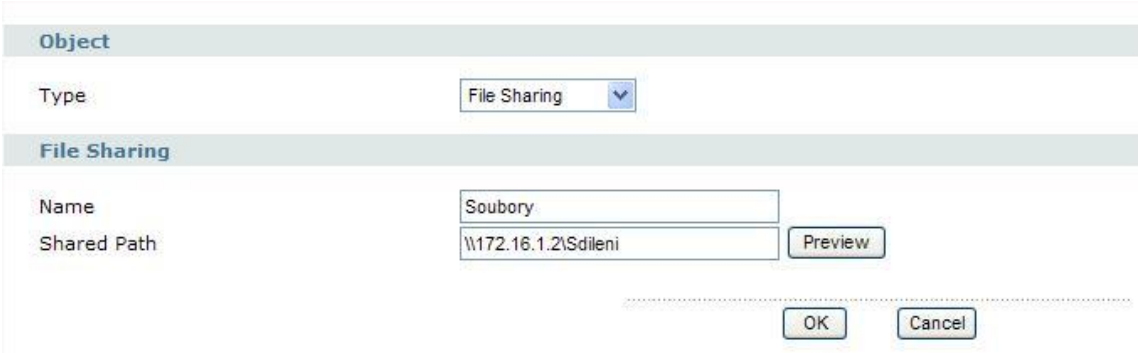
Detailní konfigurace:

Nejprve nastavím web servery a sdílené soubory pro uživatele, kteří se budou k Zywallu připojovat. Přihlásím se pod administrátorský účet a v menu vyberu Object, SSL Application. Kliknu na ikonu Add a zobrazí se okno pro konfiguraci SSL služeb. Pro webový server (obr. 3.4), nastavuji položky: Type na Web Application, Name – jméno webového serveru např. Web_Server_1, do pole URL zadám IP adresu web serveru, v mém případě server s IP adresou 172.16.1.3. Pole URL musí být vyplněno ve tvaru http://IP adresa. Dále nastavím Server Type na web server a zaškrtnu Web Page Encryption, který nedovolí uživatelům stránku uložit. Pokud bych chtěl zobrazit jinou stránku na serveru, která je uložena v podsložce, vyplním pole Entry Point. Nakonec kliknu na OK a SSL aplikace je vytvořena.



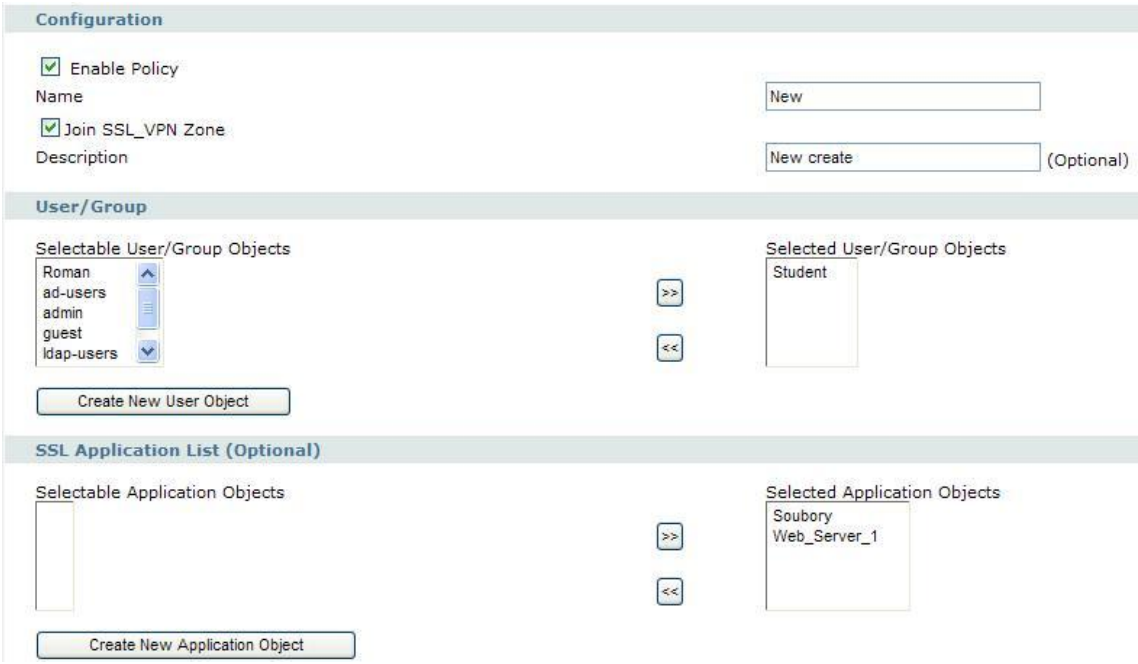
Obr. 3.4 – Konfigurace SSL služby webový server

Obdobně lze konfigurovat i server pro sdílení souborů (obr. 3.5). V menu Object, SSL Aplication kliknu na ikonu Add. V poli Type vyberu položku File Sharing, do pole Name napíšu jméno, např. Soubory a Shared Path vyplním ve tvaru \\IP adresa\sdílená složka, v mém případě \\172.16.1.2\Sdileni. Bezpečnostní brána je schopna sdílet složky, které má uživatel ve svém počítači i se systémem Windows, ale je nutno sdílení nejprve na počítači povolit. Můžeme také zvolit, zda chceme soubory pouze sdílet, nebo soubory do počítače i nahrávat. Nakonec kliknu na OK a SSL aplikace je vytvořena.



Obr. 3.5 – Nastavení serveru pro sdílení souborů

Pro konfiguraci SSL VPN kliknu na VPN, SSL VPN. Vyberu pole Access Privilege a kliknu na ikonu Add. Nyní nakonfiguruji, jaké služby budou přes webový portál dostupné a pro jaké uživatele (obr. 3.6).

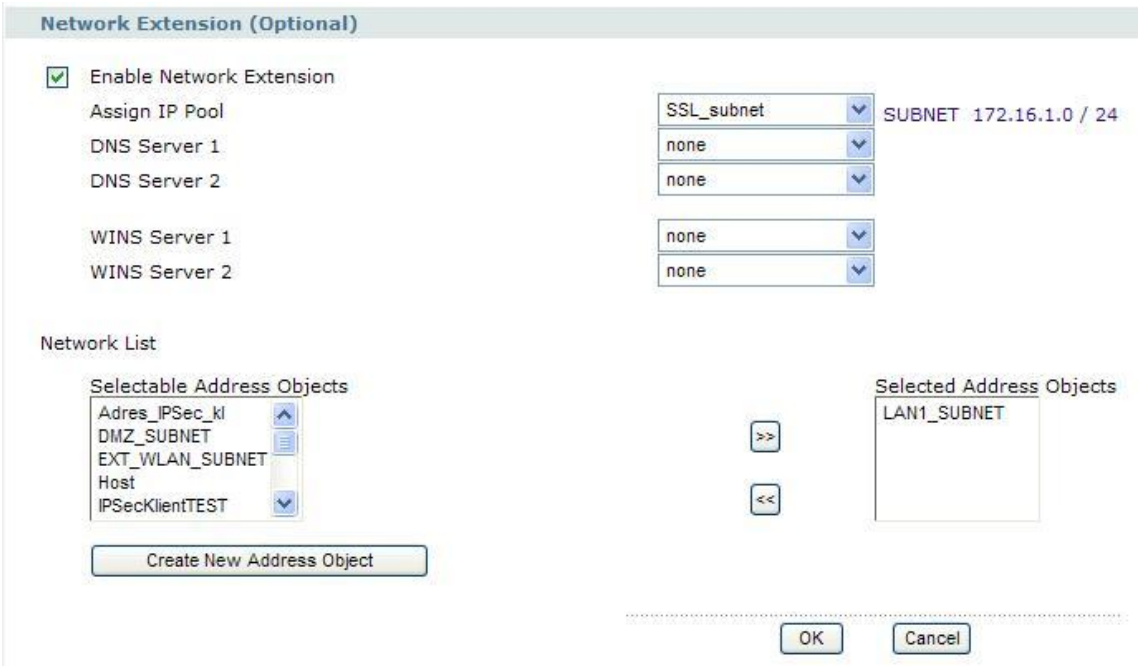


Obr. 3.6 – První část konfigurace Access Privilege

Zaškrtnu pole Enable, kterým povolím SSL VPN a pojmenuju tuto konfiguraci jako SSL_VPN. Dále zaškrtnu pole Join SSL_VPN Zone a pojmenuju jako SSL. Join SSL_VPN

Zone slouží k jednoduššímu definování politiky přístupu do této VPN sítě. V dalším kroku – User/Group využiji přednastaveného uživatele Student, kterého jsem konfiguroval v kapitole 3.1.1. Základní konfigurace bezpečnostní brány, a nastavím ho jako uživatele, který může do sítě SSL_VPN přistupovat. V SSL Application List (Optional) vyberu služby, které budou pro připojující se uživatele dostupné. Jsou to služby Web_server_1 a Soubory, které jsem konfiguroval v této kapitole na začátku detailní konfigurace.

V další části (obr. 3.7) mohu nakonfigurovat Network Extension (Optional). Tuto část konfiguruji v případě, že se bude jednat o full tunnel SSL VPN, to znamená, že uživatelé budou mít přístup nejen k definovaným službám, ale do počítače se stáhne i thin client, který umožní uživateli vstupovat i do neveřejné sítě LAN za bezpečnostní bránu. V poli Assign IP Pool zvolím rozsah IP adres, který může být uživateli přiřazen, lze zvolit i DNS a WINS servery. V části Network List zvolím, do které sítě mohou uživatelé přistupovat (LAN1_SUBNET). Kliknu na tlačítko OK a SSL VPN je nakonfigurována.



Obr. 3.7 – Druhá část konfigurace Access Privileg

Rozšířené možnosti lze nastavit ve VPN, SSL VPN, Global Settings (Obr. 3.8). Pokud chci vstupovat do neveřejné sítě LAN za Zywallem, mohu zde nastavit vstupní bránu. V mém

případě pole Network Extension Local IP nastavím na 172.16.1.100. Mohu také zvolit doménová jména pro SSL, vypsat zprávu po přihlášení a odhlášení nebo nastavit vlastní logo.

Obr. 3.8 – Global Settings

Poslední částí konfigurace SSL VPN je ověření funkčnosti. Zadám do webového prohlížeče WAN IP adresu bezpečnostní brány, v mém případě 192.168.0.2. Zobrazí se přihlašovací okno (obr. 3.9), ve kterém vyplním jméno – Student, heslo – kat440 a kliknu na SSL VPN.

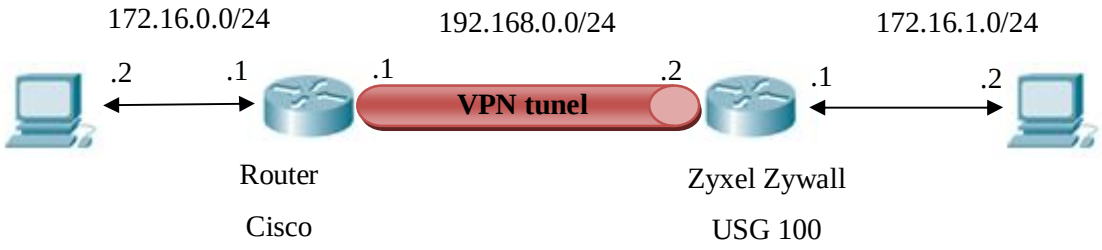
Obr. 3.9 – Přihlašovací okno

Do počítače uživatele se začne stahovat thin client a zobrazí se 2 okna. První okno s přidělenou IP adresou, maskou, DNS a WINS servery. Druhé okno (obr. 1, 2, 3 v příloze č. 1 – Přístup do SSL VPN), kde uživatel uvidí dostupné webové servery a sdílené složky pro přístup k souborům. Kliknutím na Application, Web_Server_1 se zobrazí požadovaný webový server a kliknutím na File Sharing, Soubory se zobrazí sdílené soubory. Pokud chce administrátor sledovat, kdo je připojený do SSL VPN, jaké množství dat přenesl a další informace, lze tyto údaje sledovat v bezpečnostní bráně pod VPN, SSL VPN, Connection Monitor (obr. 3.10). Správnost konfigurace můžu ověřit otevřením webového serveru Web_Server_1 a programem Wireshark. Detailní ověření i s výpisem z Wiresharku je v kapitole č. 4.

Obr. 3.10 – Sledování připojených uživatelů

3.3. IPSec VPN tunel mezi 2 routery

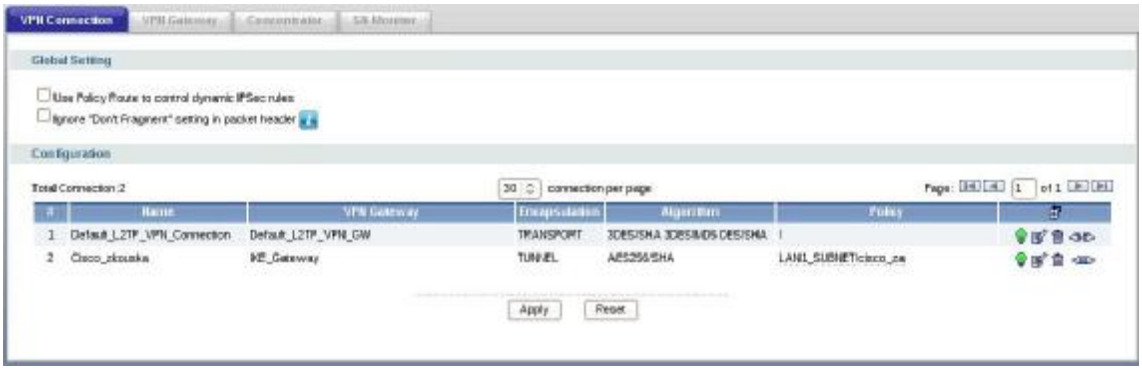
Cílem této úlohy je vytvořit bezpečné spojení mezi dvěma pobočkami. V této kapitole nebudu propojovat firemní pobočky, kde se tento typ VPN nejvíce využívá, ale využiji zařízení v laboratoři ve škole. Každá bezpečnostní brána je v reálném prostředí připojena k internetu a za nimi se nachází různé firemní servery a stanice. V této úloze se nešifruje veškerý provoz, ale pouze provoz mezi dvěma privátními sítěmi. Potenciální zaměstnanci si takto mohou bezpečně vyměňovat informace přes internet bez speciálního softwaru a konfigurace počítače. Nastavení jsem prováděl podle situace na obr. 3.11. Aby bylo možné tunel sestavit, musí všechny parametry konfigurace VPN být na obou stranách stejné. Dříve, než nakonfiguruji VPN tunel, je dobré ověřit ve firewallu a směrovací tabulce, zda mají počítače k vzdálené síti přístup i bez VPN.



Obr. 3.11 – IPSec VPN mezi 2 routery

Detailní konfigurace:

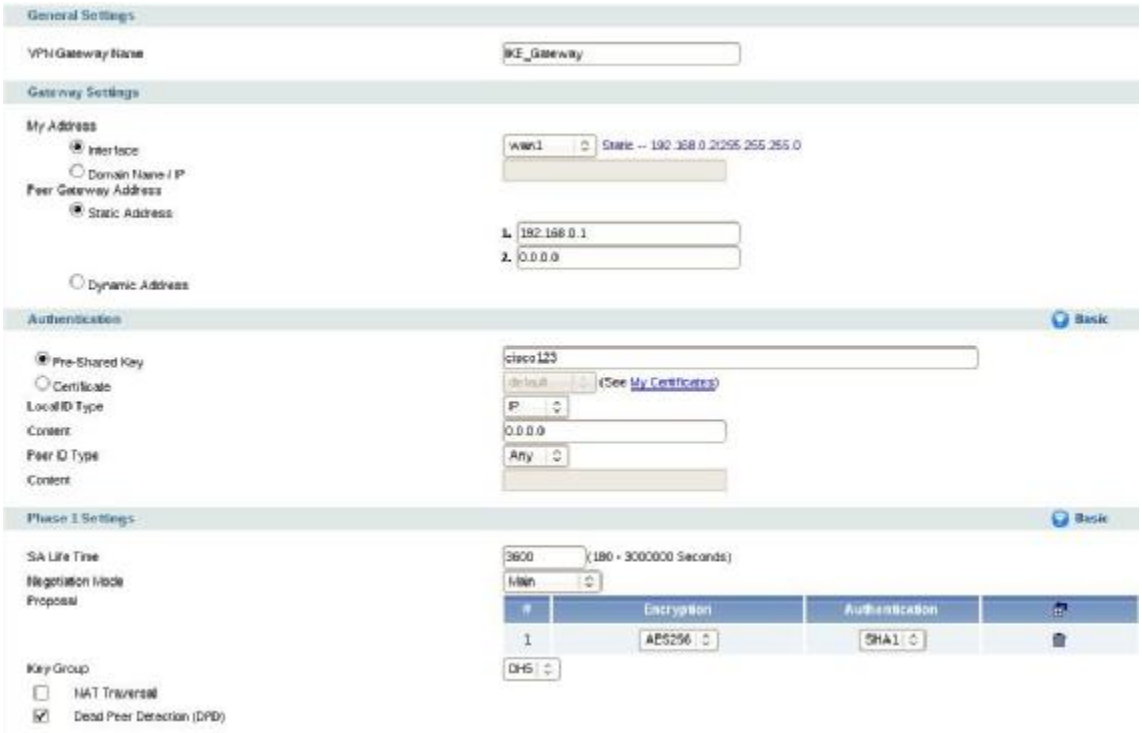
V hlavní nabídce bezpečnostní brány zvolím VPN, IPSec VPN. Zobrazí se okno pro konfiguraci VPN. V této nabídce (obr. 3.12) jsou další čtyři možnosti výběru: VPN Connection, VPN Gateway, Concentrator, SA Monitor. VPN Connection a VPN Gateway slouží k základnímu nastavení VPN, Concentrator slouží k propojení různých VPN do jedné zabezpečené sítě, v SA Monitor mohu sledovat uživatele, kteří se připojili k VPN. V další části lze zvolit, zda chci pro dynamicky vytvářený IPSec tunel využít směrování a přesně definovat cílovou adresu, nebo zda chci fragmentovat pakety větší než je MTU. Tyto volby lze zapnout nebo vypnout zaškrtnutím polí Use Policy Route to control dynamic IPSec rules a Ignore „Don´t Fragment“ setting in packet header.



Obr. 3.12 – VPN Connection

Základní konfigurace VPN mezi dvěma routery se skládá ze dvou částí. Nejprve kliknu na VPN, IPSec VPN, VPN Gateway a tlačítko Add. Zobrazí se okno pro nastavení VPN Gateway (obr. 3.13). Zvolím název, v mém případě IKE_Gateway. Dále zvolím interface, přes

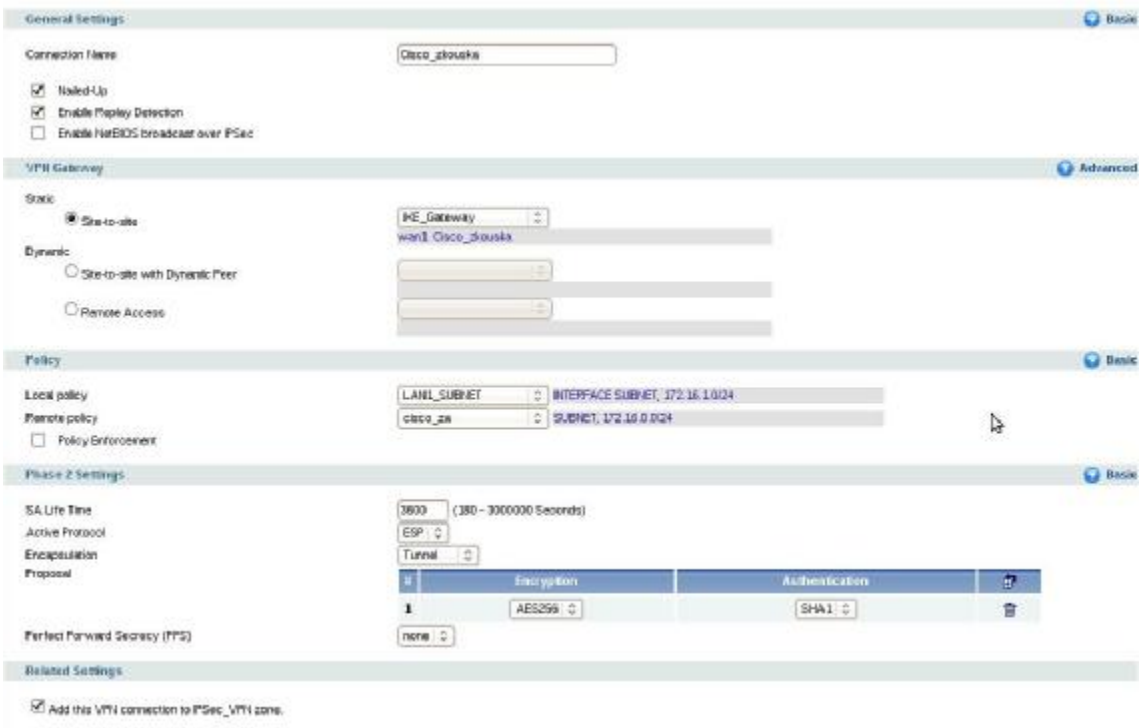
který bude VPN tunel vytvořený. Jelikož nepoužívám doménové jméno, ale IP adresu, zvolím v Gateway Settings, My Address, Interface a wan1. Směrovač na druhé straně VPN tunelu má statickou IP adresu, proto ve volbě Peer Gateway Address zvolím Static adress a zapíšu IP adresu protější strany tunelu – 192.168.0.1. Tunel bude využívat předsdílený klíč, v Authentification zvolím Pre-Shared Key a zadám klíč – cisco123. V Phase 1 Settings zvolím parametry pro IKE fázi 1. SA Life Time na např. 3600, Negotiation Mode na Main, šifrovací algoritmus jsem zvolil AES256, pro autentizaci SHA1 a Key Group DH5. Pokud by tunel procházel přes NAT, zaškrtnu pole NAT Traversal. Nakonec polem Dead Peer Detection (DPD) zvolím, že bezpečnostní brána před výměnou informací protokolu IKE zjistí připravenost vzdálenou routeru. Kliknu na OK a dále na žárovku, která zezelená a na OK. Tímto je nastavení VPN Gateway hotovo.



Obr. 3.13 – VPN Gateway pro IPSec mezi 2 routery

Druhý krok této konfigurace provedu ve VPN, IPSec VPN, VPN Connection. Kliknu na tlačítko Add a zobrazí se okno (obr. 3.14). V Connection name pojmenuju toto spojení jako Cisco_zkouska, nechám zatrženu funkci Nailed-Up a Enable Replay Detection, kterou zvolím, že bezpečnostní brána bude automaticky znovu vyjednávat IPSec SA, když vyprší časovač,

respektive zvolím aby Zywall detekoval a odmítnul staré nebo duplikované pakety. Přenášet informace NetBIOS nepotřebuji, proto nechám pole nezaškrtnuté. Jelikož toto spojení bude mezi dvěma routery s pevnými IP adresami, zvolím ve VPN Gateway Site-to-site a vyberu již nakonfigurovanou IKE_Gateway. V dalším kroku nastavím politiku přístupu. Do Policy, Local Policy zvolím podsíť LAN s rozsahem 172.16.1.0/24, je to síť do které bude směrován provoz z VPN tunelu, ale už nebude šifrovaný. Do Remote Policy zvolím podsíť, do které chci bezpečně přistupovat, v mém případě nakonfiguruji nový objekt, který pojmenuju Cisco_za a zvolím rozsah 172.16.0.0/24. V možnostech Phase 2 zvolím SA Life Time na 3600, Active Protokol na ESP, Encapsulation na Tunnel šifrovací algoritmus na AES256 a autentizaci SHA1. Diffie – Hellmanovy klíče v této fázi používat nebudu, proto Perfect Forward Secrecy nastavím na none. Z doporučeného nastavení nechám zatrhnuto Add this VPN connection to IPSec_VPN zone. Kliknu na tlačítko OK a VPN spojení je připraveno.



Obr. 3.14 – VPN Connection pro IPSec mezi 2 routery

Nyní stačí aktivovat toto VPN spojení kliknutím na žárovku, která zezelená a dále kliknout na obrázek zásuvky. Pokud jsou všechny parametry na obou stranách stejné, dojde k vyjednání IPSec SA a vytvoření VPN tunelu. Spojení můžeme ověřit tím, že oba konce

zásuvky jsou spojeny (obr. 3.12) ve VPN Connection, nebo na úvodní obrazovce – Status – VPN Status. Pokud dojde během vyjednávání k chybě, mohu se podívat do Maintanance, Log, kde je celý proces vyjednávání tunelu zachycen.

V této chvíli je tunel vytvořen, ale není možné komunikovat z počítače v jedné síti s počítačem v druhé síti. Předpokládám, že router Cisco je správně nastaven, proto musím nastavit správné směrování na bezpečnostní bráně Zywall. Zvolím Network, Routing, Police Routing (obr. 3.15) a tlačítkem Add přidám další záznamy. Nejprve řádek č. 1, kterým bráně určím, aby veškerý provoz, který přijde z VPN tunelu Cisco_zkouska, směroval do mé sítě LAN. Druhým řádkem určím, aby provoz, který přijde z portu lan1 se zdrojovou adresou mého LAN subnetu – 172.16.1.0/24 a s cílovou adresou sítě, která je za Ciscem posílal do VPN tunelu Cisco_zkouska. V této chvíli je vše nastaveno a síť je plně funkční.

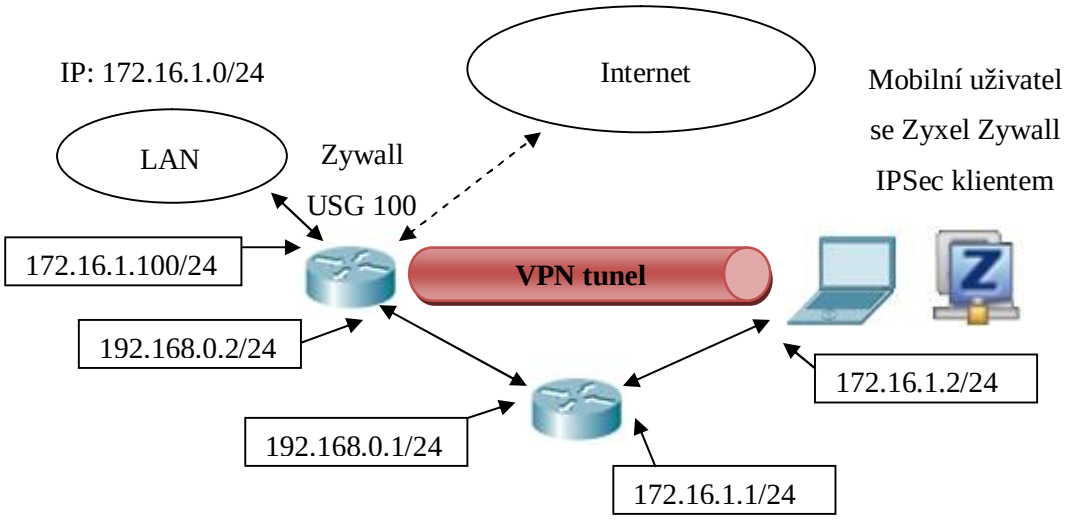
Obr. 3.15 – Nastavení Policy Route pro VPN mezi 2 routery

Nyní mohu VPN spojení otestovat. Pracoval jsem v laboratoři, proto jsem mezi routery připojil hub, ke kterému jsem také připojil počítač s programem Wireshark. Nejjednodušším způsobem jak otestovat tuto konfiguraci je ping. Proto jsem vyslal ping ze sítě 172.16.0.0 počítač v síti 172.16.1.0. Jak je dále popsáno v kapitole č. 4, data jsem zachytil, ale jsou šifrovaná a pro potenciálního útočníka téměř nepoužitelná.

3.4. IPSec VPN tunel mezi Zywall USG 100 a Zyxel Zywall IPSec klientem

V této části propojím VPN tunelem bezpečnostní bránu Zywall USG 100 a mobilního uživatele, který má nainstalován speciální software pro vybudování IPSec VPN tunelu. Opět si lze představit tuto konfiguraci ve firmě. Zywall je centrální prvek, za kterým se nachází různé

firemní servery a stanice. Také je vhodné pro tuto konfiguraci připravit webový server (Apache v systému linux) a počítač s nastaveným sdílením souborů jako souborový server. Koncový uživatel se může připojit odkudkoliv, neznám jeho IP adresu. Zywall lze nastavit tak, aby šifroval a do tunelu posílal provoz, který je určen pouze pro LAN síť za bezpečnostní branou, nebo šifrovat veškerý provoz a do sítě internet budu vstupovat přes Zywall (obr. 3.16). Uživatel tímto využívá veřejnou IP adresu bezpečnostní brány a je chráněn jejím firewallem a antivirovým programem. Jelikož je konfigurace velmi podobná jako kapitola 3.3. IPSec VPN tunel mezi dvěma routery, budu se zde s některými obrázky odkazovat. Nevýhodou pro tuto úlohu je pouze 30 denní licence pro program Zywall IPSec klient. Program je vázán na fyzickou adresu počítače a po 30 dnech je nutné program zakoupit. V rámci laboratorní úlohy není vhodné, aby studenti vstupovali na internet. Konfigurace i testování bude probíhat lokálně, ale bezpečnostní brána bude připravena pro šifrování veškerého provozu.



Obr. 3.16 – VPN tunel mezi Zywall USG 100 a mobilním uživatelem

Detailní konfigurace:

V první části nastavím VPN_Gateway obdobně jako na obr. 3.13. Kliknu na VPN, IPSec VPN, VPN Gateway, Add a do pole VPN Gateway Name zadám název IPSec_kl, v Gateway Settings vyberu My Address, Interface, wan1 – 192.168.0.2. Jelikož nevím, z jaké IP adresy se bude klient připojovat, v poli Peer Gateway Address zvolím Dynamic Address. Pro Authentification jsem zvolil Pre-Shared Key vsbkat440. Ostatní hodnoty v tomto poli pro mě

nejsou podstatné, protože nevyužívám certifikáty. Dále zvolím parametry pro IKE fázi 1. SA Life Time jsem zvolil 3600, Negotiation Mode – Main, Encryption – DES, Authentication – MD5, Key Group – DH1. Opět jsem zaškrtnul NAT Traversal a odškrtnul Dead Peer Detection (DPD). Pro bezpečnější spojení bude ještě brána vyžadovat další ověření, které nastavím kliknutím na More Settings a v Extended Authentification označím Enable Extended Authentification a hodnotu zvolím na default. Tímto bráně zadám, aby při spojení vyžadovala uživatelské jméno a heslo, které bude hledat v lokální databázi uživatelů. Mohu zde využít předdefinovaného uživatele Student s heslem kat440, které budu zadávat do IPSec Zywall VPN klienta. Kliknu na tlačítko OK, žárovku, která zezelená a opět na tlačítko OK. Tímto je VPN Gateway připravena.

V druhé části nastavím VPN Connenction. Kliknu na VPN, IPSec VPN, VPN Connection, Add a do pole Connection Name zadám IPSec_Zyxel_klient. Ostatní možnosti u General Settings nechám neoznačené. Ve VPN Gateway zvolím Site-to-site with Dynamic Peer a do VPN Gateway vyberu již nastavenou bránu IPSec_kl. Pokračuji nastavením politiky přístupu. V Policy, Local Policy vytvořím objekt, který bude mít rozsah IP adres 0.0.0.0 – 255.255.255.255. Tímto zajistím, aby veškerý provoz byl šifrován a poslán do VPN tunelu. Pokud bych provoz do internetu nechtěl posílat přes VPN tunel a bezpečnostní bránu, ale přímo přistupovat na internet a šifrovat pouze provoz do místní sítě LAN za Zywallem, zvolím zde rozsah pro LAN1 – 172.16.1.0/24. Abych oddělil IP adresy lokální sítě a uživatelů s VPN klientem, zadám do Remote Policy objekt s adresou 172.16.200.1/32. Policy Enforcement nezaškrtnu. V nastavení Phase 2 Settitngs zvolím SA Life Time – 3600, Active Protocol – ESP, Encapsulation – Tunnel, Encryption – DES, Authentication – MD5 a Perfect Forward Secrecy (PFS) zvolím none. Zaškrtnu Add this VPN Connection to IPSec_VPN zone, kliknu na OK a kliknutím na žárovku, která zezelená je nastavení dokončeno.

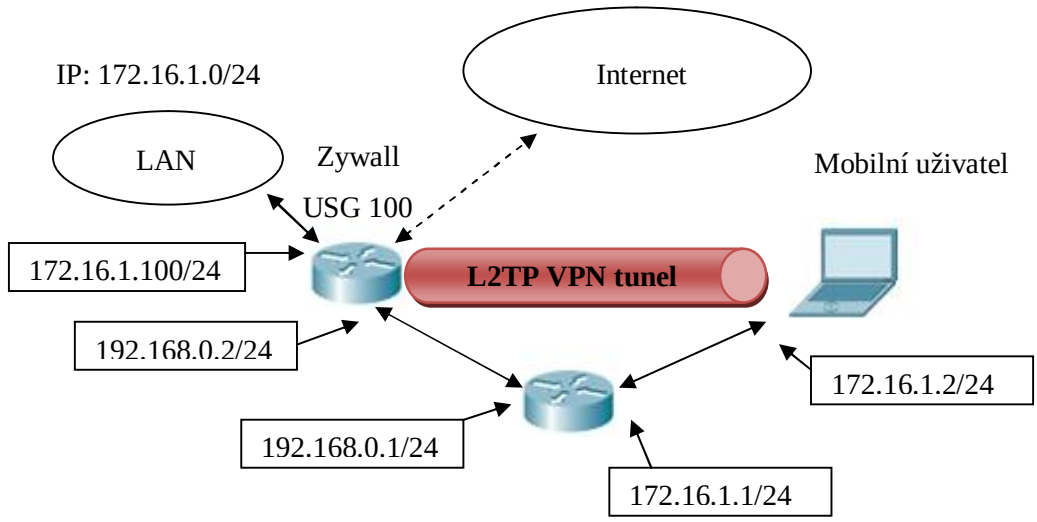
Aby bylo nastavení korektní, je potřeba nastavit směrování na internet (pokud se bude připojení k internetu využívat). Kliknu na Network, Routing, Policy Route a určím Zywallu, aby provoz, který přijde z VPN sítě jménem IPSec_VPN_klient z jakoukoliv zdrojovou i cílovou IP adresou směroval na port wan1. Nastavení provedu podle obr. 3.17 – 1. řádek.

Obr. 3.17 – Směrování pro IPSec klienta a L2TP

Poslední část je otestování správnosti konfigurace. Na stránce www.zyxel.com je k dispozici zkušební verze IPSec klienta. Soubor stáhnu, nainstaluji a přesvědčím se, že služba IPSec je v nastavení služeb ve Windows vypnuta. Podle přílohy č. 2 nastavím Zyxel Zywall IPSec VPN klienta a kliknu na open tunnel. Dojde k vyjednání všech parametrů a otevření VPN tunelu. Mohu vyslat dotaz na webový server, který je v lokální síti za Zywallem, nebo stáhnout soubor ze souborového serveru a sledovat ve wiresharku provoz. Veškerý provoz mezi bezpečnostní branou a uživatelem je šifrován. Pokud by byl Zywall připojen k internetu, uživatel by vystupoval na internet pod veřejnou IP adresou Zywallu. Detailní vyhodnocení je v kapitole č. 4.

3.5. L2TP VPN tunel mezi Zywall USG 100 a klientem

V této úloze vytvořím L2TP tunel mezi bezpečnostní branou a mobilním klientem. L2TP je VPN síť, která pracuje na 2. vrstvě OSI modelu a chová se podobně jako připojení se Zyxel Zywall IPSec VPN klientem. V privátní síti je podobně jako v kapitole 3.4. nastaven webový a souborový server. K připojení využiji nastavení připojení k síti ve Windows, kde lze nakonfigurovat VPN síť přes L2TP nebo PPTP. Při této konfiguraci je také důležité, aby služba IPSec ve Windows byla zapnuta. Dle obr. 3.18 budu stejně jako v kapitole 3.4. přistupovat přes VPN jak do vnitřní sítě LAN za bezpečnostní branou, tak i na internet, pokud bude připojen. V rámci laboratorní úlohy připojení k internetu nebudu využívat, ale bezpečnostní brána bude pro tento způsob přístupu připravena.



Obr. 3.18 – Scénář pro L2TP

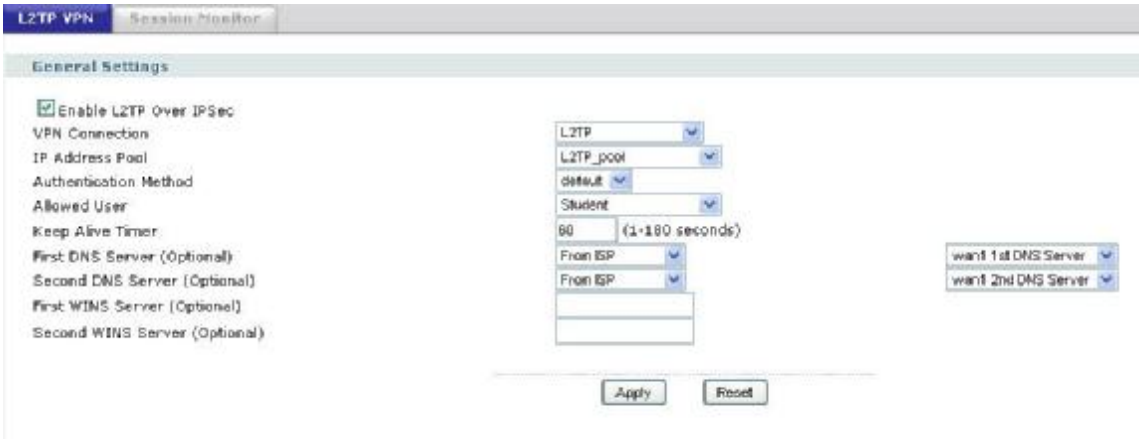
Detailní konfigurace:

První dva kroky jsou obdobné jako u konfigurace IPSec tunelu mezi Zywall USG 100 a Zyxel Zywall IPSec klientem. Kliknu na VPN, IPSec VPN, VPN Gateway, Add a do pole VPN Gateway Name zadám název L2TP_GW, v Gateway Settings vyberu My Address, Interface, wan1 – 192.168.0.2. Jelikož nevím, z jaké IP adresy se bude klient připojovat, v poli Peer Gateway Address zvolím Dynamic Address. Pro Authentification jsem zvolil Pre-Shared Key vsbkat440. Ostatní hodnoty v tomto poli pro mě nejsou podstatné, protože nevyužívám certifikáty. Dále zvolím parametry pro IKE fázi 1. SA Life Time jsem zvolil 3600, Negotiation Mode – Main, Encryption – 3DES, Authentication – SHA1, Key Group – DH2. Opět jsem zaškrtnul NAT Traversal a Dead Peer Detection (DPD). Kliknu na tlačítko OK, žárovku, která zezelená a opět na tlačítko OK. Tímto je VPN Gateway připravena.

V druhé části nastavím VPN Connenction. Kliknu na VPN, IPSec VPN, VPN Connection, Add a do pole Connection Name zadám L2TP. Ostatní možnosti u General Settings nechám neoznačené. Ve VPN Gateway zvolím Site-to-site with Dynamic Peer a do VPN Gateway vyberu již nastavenou bránu L2TP_GW. Pokračuji nastavením politiky přístupu. V Policy, Local Policy vytvořím objekt (Interface IP), který bude odpovídat IP adrese WAN rozhraní – 192.168.0.2. Do Remote Policy vytvořím další objekt (Host) s adresou 0.0.0.0. Policy Enforcement nezaškrtnu. V nastavení Phase 2 Settitngs zvolím SA Life Time – 3600, Active Protocol – ESP, Encapsulation – Transport, Encryption – 3DES, Authentication – SHA1 a

Perfect Forward Secrecy (PFS) zvolím none. Nezaškrtnu Add this VPN Connection to IPSec_VPN zone, kliknu na OK a kliknutím na žárovku, která zezelená je nastavení dokončeno.

IPSec parametry jsou nastaveny, ale chybí ještě nastavit parametry pro L2TP (obr. 3.19). Kliknu na VPN, L2TP VPN. Zaškrtnu Enable L2TP Over IPSec, čímž zapnu L2TP. Do pole VPN Connection vyberu konfiguraci z IPSec VPN, VPN Conection – L2TP. Do Address Pool vytvořím nový objekt, který bude obsahovat IP adresy přistupujícího uživatele – 172.16.1.1 – 172.16.1.254 a pojmenuju jej L2TP_pool. Authentification Method ponechám default, Allowed User – uživatel, který bude přes L2TP přistupovat bude student, kterého jsem konfiguroval v kapitole 3.1.1. Pro přístup na internet zvolím i první a druhý DNS server v poli First DNS Server (Optional) a Second DNS Server (Optional) a zvolím wan1 1 st DNS server, respektive wan1 2 nd DNS server. Kliknu na tlačítko OK a VPN přístup je nakonfigurován.



Obr. 3.19 – Konfigurace L2TP

Nastavení přístupu je hotovo, v další části nastavím směrování a přístup na internet (pokud se bude připojení k internetu využívat). Kliknu na Network, Routing, Policy Route a přidám dvě nová pravidla (obr. 3.17). Nejprve pravidlo č. 2, kterým bráně zadám, aby veškerý provoz, který bude mít cílovou IP adresu 172.16.1.1 – 172.16.1.254 (L2TP_pool) směroval do L2TP tunelu (L2TP). Tímto je zajištěn šifrovaný přístup do místní sítě LAN. Pravidlem č. 3 zajistím přístup na internet. Provoz, který přijde z L2TP tunelu se zdrojovou IP adresou L2TP_pool a jakoukoliv cílovou adresou pošle brána na port wan1 neboli WAN_TRUNK.

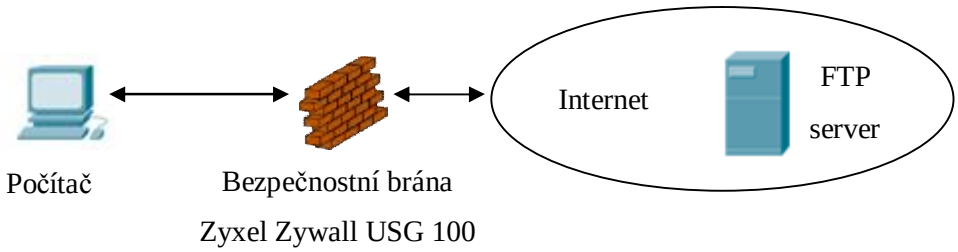
Poslední částí je ověření správnosti konfigurace. Dle přílohy 3 nastavím ve Windows připojení k firemní síti přes VPN. Po nastavení všech parametrů dojde k vytočení tunelu a k připojení k bezpečnostní bráně. Na počítači, který se k bezpečnostní bráně připojuje, zapnu

program wireshark. Spustím webový prohlížeč a zadám jakýkoliv webový server na internetu nebo ve firemní síti. Veškerý provoz je v tomto případě šifrován. Ve VPN, L2TP VPN, Session Monitor mohu sledovat připojené uživatele. Detailní rozbor provozu je v kapitole č. 4.

3.6. Firewall

Firewall slouží k omezení provozu pro různé služby. Tato laboratorní úloha je zaměřena na ověření funkčnosti firewallu. V továrním nastavení bezpečnostní brány je definováno několik pravidel pro přístup. Pro SSL VPN je důležité, aby bylo vypnuto pravidlo, které zakazuje přístup z internetu (wan portu) na administraci Zywallu. Po vypnutí tohoto pravidla se dostanou uživatelé k SSL VPN, ale také umožním přístup hackerům. Tito lidé skenují IP adresy a snaží se dostat do privátní sítě za bezpečnostní bránu, nebo na této bráně prolomit přihlašovací údaje. Proto pokud uživatelé přistupují k privátní síti ze statických IP adres je vhodné přístup omezit těmito statickými IP adresami.

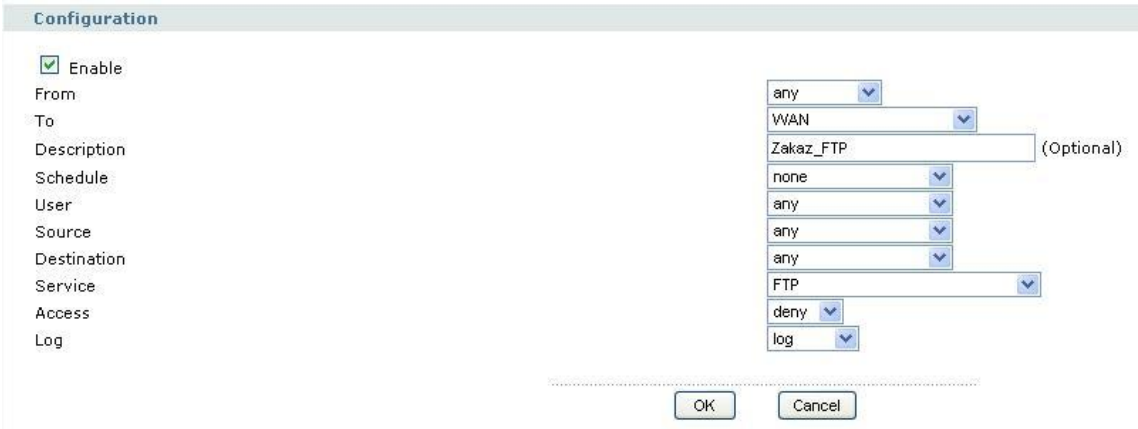
Jako příklad konfigurace pro firewall uvedu jedno pravidlo a to zakázaní FTP z místní sítě na internet (obr. 3.20), nebo lze připojit k wan portu přímo ftp server (např. ftp server v linuxu) a testovat pravidlo lokálně. Připojím bezpečnostní bránu k internetu a k portu LAN1 připojím minimálně 1 počítač. Pokud bude chtít uživatel z privátní sítě přistupovat na FTP server na internetu, bezpečnostní brána provoz pro tuto službu zablokuje a vytvoří záznam v logu.



Obr. 3.20 – Schéma pro konfiguraci firewallu

Dle obr. 3.21 mohu nakonfigurovat pravidla pro firewall. Zvolím, z kterého interfacu (From) na který (To) se bude provoz filtrovat. Na výběr jsou hardwarové porty bezpečnostní brány (LAN, WAN, DMZ…) i SSL a IPSec tunely, které jsem vytvořil. V poli Description

mohu pravidlo popsat, mohu definovat, v jakém časovém období bude pravidlo platné (Schedule) a uživatelé, kteří budou pravidlo využívat (User). Dále lze zvolit zdrojovou a cílovou IP adresu (Source, Destination), podsítě nebo rozsah IP adres, pro které bude pravidlo platné. V poli Service vyberu službu, kterou chci zablokovat nebo povolit. Pokud nestačí předem nakonfigurované služby, lze vytvořit vlastní objekt a porty nebo rozsah portů definovat manuálně. V poslední části zvolím, zda chci provoz přes Zywall propustit nebo zablokovat (Access) a lze také zvolit, jestli chci využití tohoto pravidla zapisovat do logu (Log). V tomto případě pokud uživatel využije pravidlo, zapíše se zpráva do logu. Kliknutím na tlačítko OK a poté na symbol žárovky, která zezelená, se pravidlo aktivuje.



Obr. 3.21 - Firewall

Konfiguraci firewallu mohu otestovat například připojením na FTP server ftp://ftp.zyxel.com/. Připojení na server se nezdaří a do logu bezpečnostní brány se zapíše údaj o pokusu připojení k FTP serveru (obr. 3.22). Z logu lze vyčíst datum a čas pokusu o připojení, zdrojovou a cílovou IP adresu, zda byl provoz zablokován nebo povolen a další méně podstatné informace.

Obr. 3.22 – Log firewallu

4. Vyhodnocení různých konfigurací

SSL VPN nabízí jednoduchý přístup pro koncové uživatele. Stačí znát správnou IP adresu, uživatelské jméno a heslo a uživatel se může připojit odkudkoliv. Při tomto způsobu připojení nepotřebuje žádný speciální software ani složité konfigurování služeb. Uživatel si vystačí pouze s webovým prohlížečem a získá při full tunnel módu plný přístup do privátní sítě za bezpečnostní branou. Může využít jak firemní webové, e - mailové, souborové či jakékoliv jiné servery, ale také přímý přístup k pracovním stanicím. SSL VPN nešifruje veškerý provoz, ale pouze provoz, který směřuje do lokální sítě za bezpečnostní bránu, tzn. provoz na internet odchází nešifrován, klasicky přes uživatelova poskytovatele internetu.

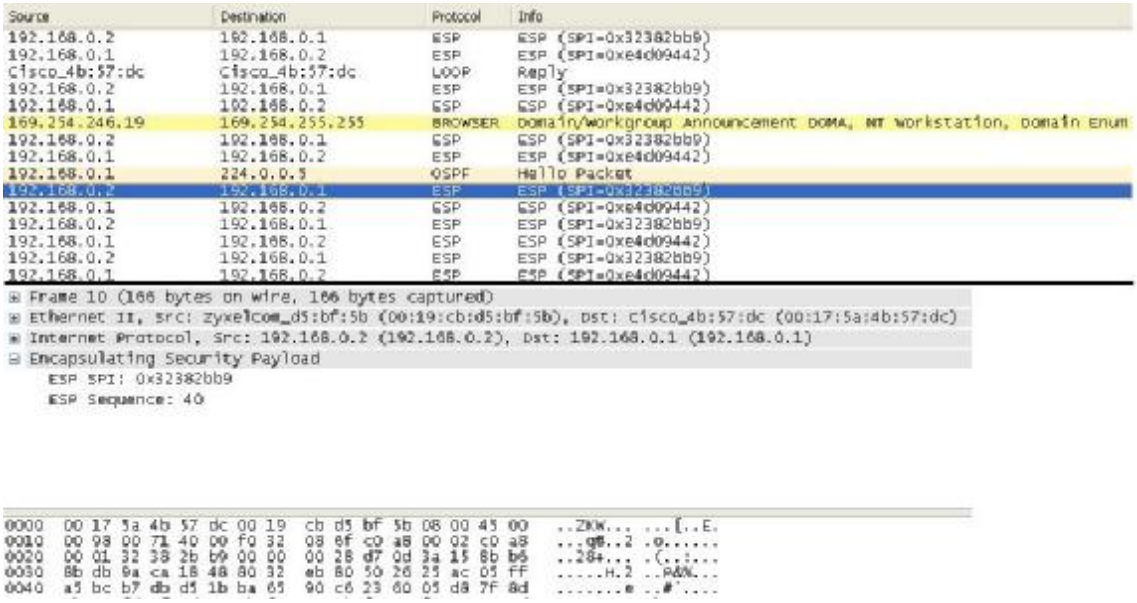
Při konfiguraci IPSec VPN tunelu jsem mezi dvěma routery využil šifrování AES a při Zyxel Zywall IPSec klientovi jsem použil DES. AES je dnes nejbezpečnější šifrovací algoritmus a doporučuje se jej využívat, pokud je dostupný. V obou případech je šifrován provoz do privátních sítí, při použití IPSec klienta i na internet. To znamená, že uživatel nevstupuje na internet pod svou veřejnou IP adresou, ale pod IP adresou bezpečnostní brány Zyxell Zywall USG 100. Konfigurace s Zywall IPSec klientem je velmi podobná konfiguraci L2TP. Ale Zywall IPSec klient nabízí průhlednější konfiguraci, lze zvolit transportní, nebo tunelovací mód, na výběr jsou všechny dostupné šifrovací a autentizační algoritmy jako u bezpečnostní brány, lze využít i certifikáty. Koncový uživatel nemusí prakticky nic konfigurovat. Administrátor může vygenerovat ve svém Zyxel VPN klientovi konfigurační soubor na míru každému uživateli a ten odeslat např. e-mailem. Uživateli pak stačí, když si software nainstaluje, zadá licenční klíč a importuje konfigurační soubor. Nevýhodou u tohoto řešení je, že software je placený a je potřeba zakoupit licenci zvlášť pro každý počítač, který bude tento typ spojení využívat.

L2TP přístup lze nakonfigurovat přímo ve Windows a není potřeba platit ani instalovat další software. V tomto případě stejně jako u Zywall IPSec VPN klienta je veškerý provoz šifrován. Nevýhodou je, že L2TP vyžaduje méně bezpečný transportní mód a konfigurace na straně uživatele může být složitější.

Při konfiguraci jednotlivých přístupů musí administrátor také zvážit, jaký zvolit šifrovací algoritmus. AES je nejbezpečnější způsob šifrování, můžeme zvolit 128, 192 nebo 256 bitů. Na druhou stanu musí promyslet, kolik VPN tunelů může být najednou vytvořeno, protože šifrování AES je výpočetně náročné a při více VPN tunelech nemusí zbývat volný výkon

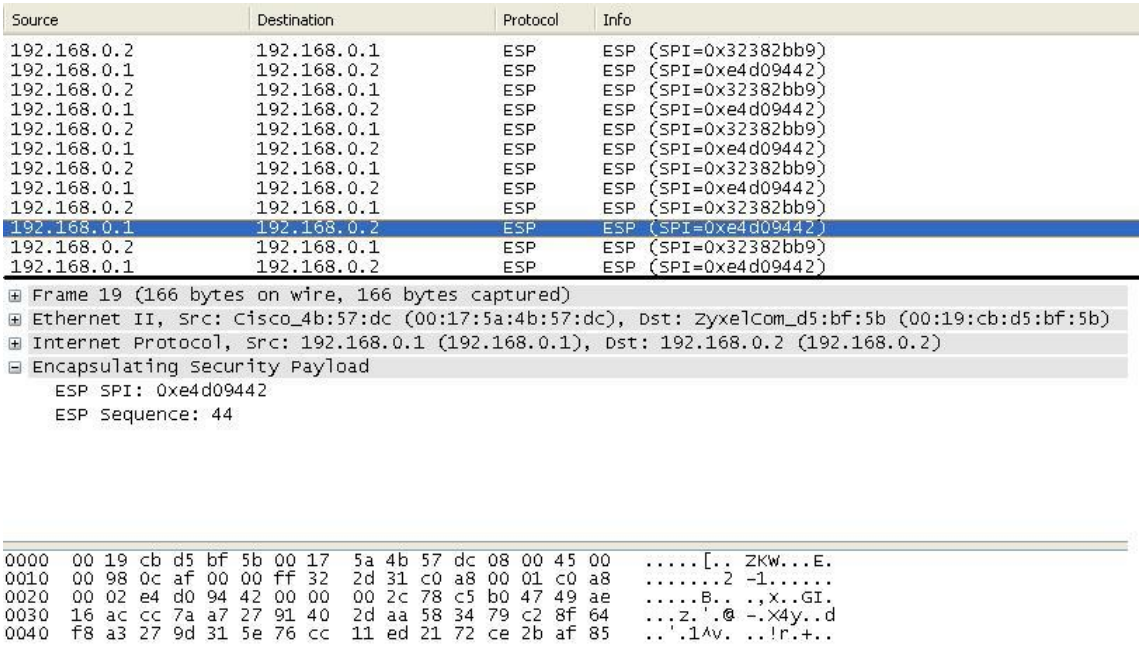
procesoru pro ostatní uživatele. V takovémto případě je vhodné zvolit méně bezpečné šifrování DES nebo 3DES.

Na ukázku šifrování jsem v programu Wireshark zachytil provoz pro konfiguraci mezi dvěma routery (obr. 4.1). V tomto případě se šifruje pouze provoz mezi sítěmi, které jsou za bezpečnostními branami. Konfigurace využívá IPSec tunel a šifrování AES256. Jediné, co může potenciální útočník v tomto případě odchytit, je šifrovaný provoz zapouzdřený do protokolu ESP. Útočník tedy vidí pouze zdrojovou a cílovou IP adresu, SPI a číslo ESP sekvence. Ze zachyceného provozu lze také vysledovat nezabezpečený ostatní provoz (OSPF, LOOP…).



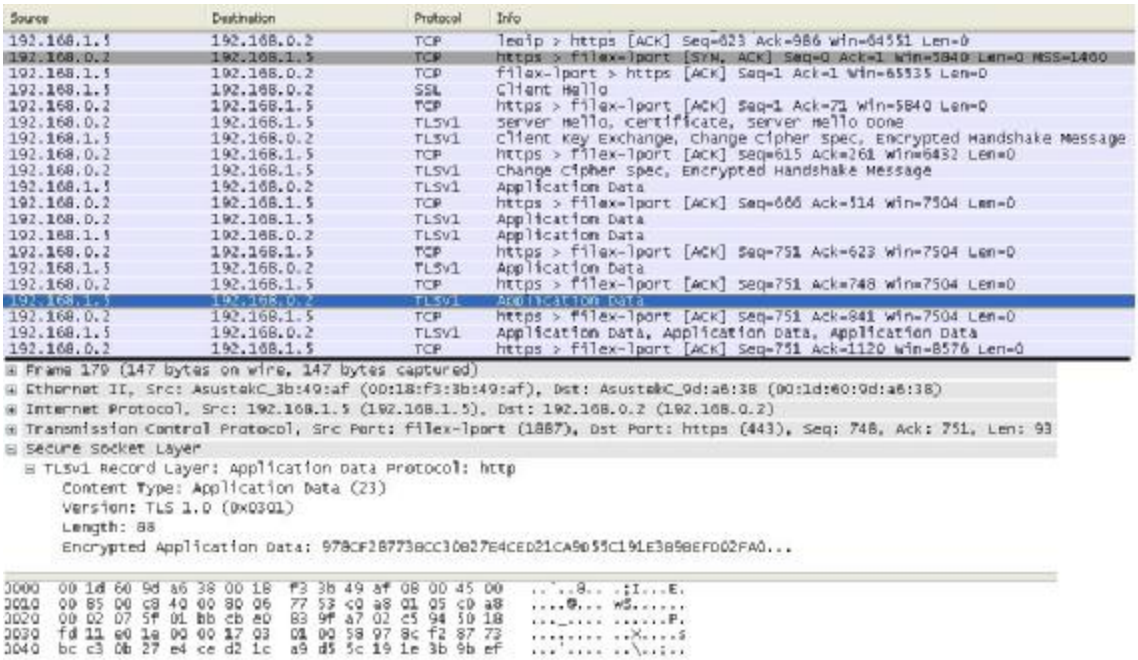
Obr. 4.1 – Zachycení provozu pro IPSec tunel – ping z 192.168.0.2 na 192.168.0.1

Podobný provoz (obr. 4.2) lze zachytit i pro konfiguraci IPSec VPN tunel mezi bezpečnostní branou a Zyxell Zywall IPSec klientem a pro konfiguraci s L2TP protokolem. V těchto dvou případech je zde ještě jedna velká výhoda. V těchto konfiguracích útočník nepozná skutečnou cílovou IP adresu. Cílová IP adresa může být počítač nebo server v privátní síti za bezpečnostní branou, ale i jakýkoliv server v internetu. Jedinou cílovou adresu, kterou potenciální útočník zachytí je veřejná IP adresa Zywallu v případě s připojením k internetu, privátní adresu v případě laboratorní úlohy.



Obr. 4.2 – Zachycení provozu pro L2TP a IPSec VPN se Zyxel Zywall IPSec klientem

Stejným způsobem jsem také zachytil provoz přes SSL VPN (obr. 4.3). Data jsou zapouzdřena do protokolu TLS a jediné, co může potenciální útočník vidět, jsou zašifrovaná data. Nejčastějším využitím SSL VPN jsou banky s internetovým bankovnictvím. Zde bychom zachytili obdobný provoz.



Obr. 4.3 – Provoz při SSL VPN

5. Závěr

Bezpečnostní brána Zyxel Zywall USG 100 je určena především pro domácí použití a malé kanceláře. Svými vlastnostmi komplexně zabezpečuje vnitřní síť a nabízí administrátorům širokou škálu funkcí. V této diplomové práci jsem se zaměřil na jednu z vlastností a to VPN. Pokud klient, který vycestuje např. do zahraničí, má vytvořené VPN spojení na tuto bezpečnostní bránu, může snadno přistupovat k souborům a webovým serverům, které má ve své domácí síti. Spojení je šifrované, brána využívá dnes standardně používané šifrování DES, 3DES, AES 128, 192 a 256 b. Pro autentizaci se využívají protokoly MD5 a SHA1. Ve svých konfiguracích jsem využíval předsdíleného klíče, ale existuje také možnost využít osobních certifikátů. Při správném nastavení lze šifrovat veškerý provoz a vstupovat na internet pod IP adresou této bezpečnostní brány. Této volby lze využít např. při VoIP. Uživatel se připojí ze zahraničí na bezpečnostní bránu, spustí program pro telefonování (SJPhone, X-lite) a zaregistruje se u svého poskytovatele VoIP služby. Takovýto uživatel nemusí platit za telefonní spojení ze zahraničí, ale může v rámci své země telefonovat i zdarma, pokud volaný používá také VoIP. Jedinou nevýhodou je, že musíme brát na zřetel zpoždění, které vzniká šifrováním a dešifrováním paketů.

Konfiguroval jsem 3 typy připojení přes VPN: SSL, IPSec a L2TP. Každá z těchto konfigurací má své výhody a nevýhody. Tato diplomová práce ukazuje, jak tato připojení nastavit, odzkoušet a jaké výstupy očekávat. Studenti, kteří budou mít zájem se dozvědět informace ohledně VPN, si mohou tuto diplomovou práci přečíst a dozví se tak nejen teoretické informace ohledně využívaných protokolů, ale také si mohou jednotlivé přístupy odzkoušet.

Zyxel Zywall USG 100 nabízí kromě VPN i další pokročilé služby. Jsou to především antivirová a antispamová ochrana, IDP a ADP modul. Tyto moduly dokážou spolehlivě ochránit síť před viry, neautorizovanými vstupy nebo různými druhy útoků a mohly by sloužit jako témata dalších diplomových prací. Některé tyto funkce jsou ale nabízeny ve zkušební verzi a pro případné další využití se musí dokoupit od firmy Zyxel licence.

Literatura

[Lockhart, 2005]

LOCKHART, Andrew, VESELSKÝ, Jiří. *Bezpečnost sítí na maximum*. 1. vydání. Brno: CP Books, 2005. 276 s. ISBN 80-251-0805-8

[Northcutt, 2005]

NORTHCUTT, Stephen; TRÁVNÍČEK, Miloš; KRÁSENSKÝ, David. *Bezpečnost sítí: velká kniha: Bezpečnost počítačových sítí: kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě (Variant.)*. 1. vydání. Brno: CP Books, 2005. 589 s. ISBN 80-251-0697-7

[Thomas, 2005]

THOMAS, Thomas M.; KRÁSENSKÝ, David. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vydání. Brno: CP Books, 2005. 338 s. ISBN 80-251-0417-6

[Odom, 2008]

ODOM, Wendell. *CCNA ICND2 Official Exam Certification Guide*. 2. vydání. Indianapolis, USA: Cisco Press, 2009. 690 s. ISBN 978-1-58720-181-3

Elektronická literatura

[Zywall USG 100 User's Guide]

User's Guide [online]. 2008 Dostupný z www: ftp://ftp2.zyxel.com/ZYWALL_USG_100/user_guide/ZYWALL%20USG%20100_2.20.pdf

[SSL VPN]

SSL VPN. Dostupný z www: <http://en.wikipedia.org/wiki/Secure_Sockets_Layer_virtual_private_network>

Seznam příloh